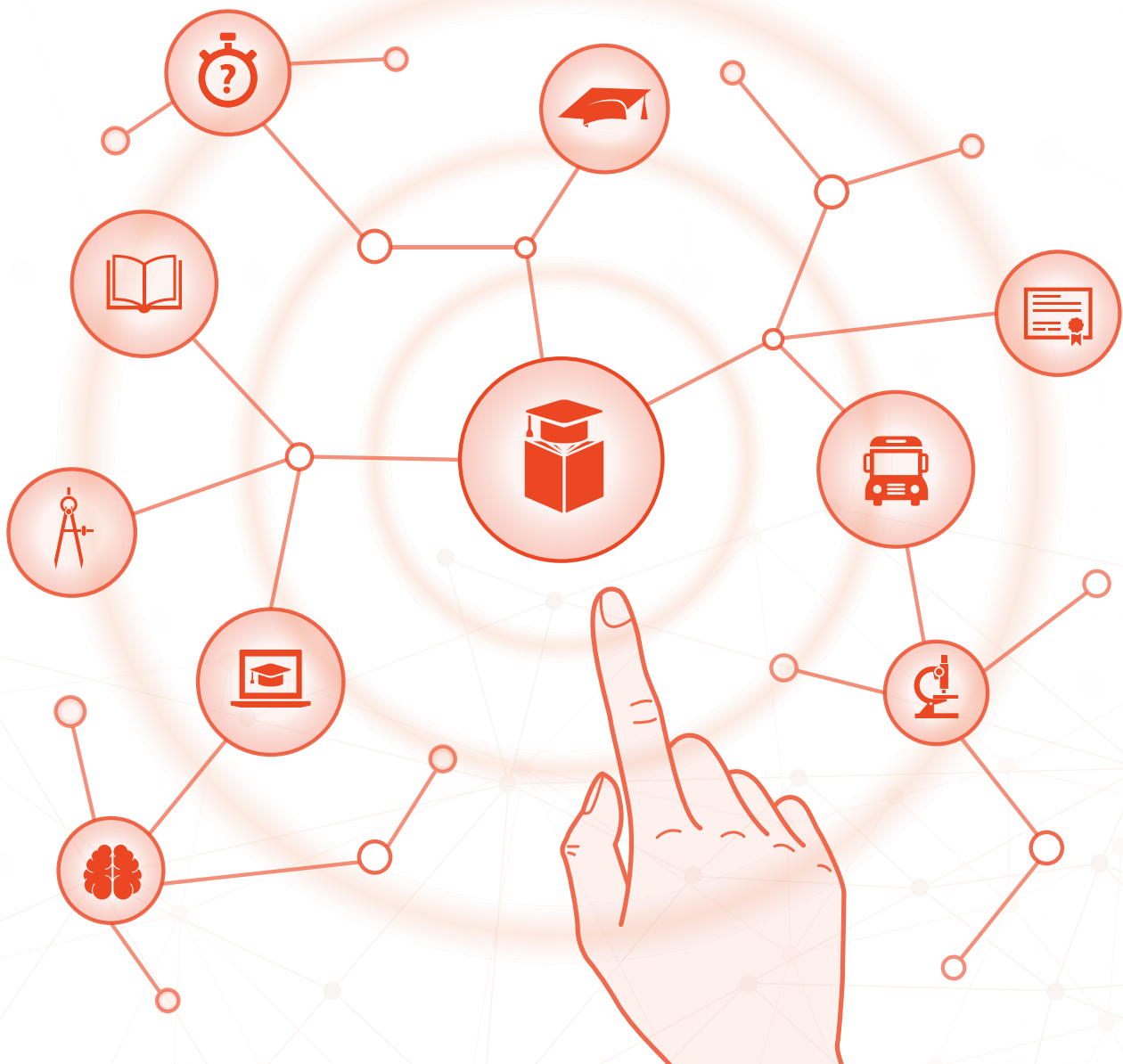




e-Readiness Assessment of Somali Higher Education Institutions 2026

Full Technical Report



Contents

List of Figures	i
List of Tables	ii
List of Abbreviations	iii
Executive Summary	v
1 Introduction and Context	1
1.1 Digital Transformation and Higher Education in Fragile Contexts -----	1
1.2 Objectives and Scope -----	2
1.3 Conceptual and Analytical Framework -----	3
1.4 Structure of the Report -----	4
2 Methodology and Assessment Framework	5
2.1 Assessment Design and Framework -----	5
2.2 Data Collection and Institutional Coverage -----	5
2.3 Data Management, Quality Assurance and Limitations -----	6
2.4 Analytical Approach and Readiness Staging -----	7
2.5 Benchmarking Approach -----	8
3 Findings by E-Readiness Domain	9
3.1 Profile of Participating Institutions -----	9
3.1.1 Distribution of institutions by size -----	9
3.1.2 Distribution of student enrolment by institutional size -----	10
3.1.3 Institutional type -----	11
3.2 ICT Infrastructure and Systems -----	12
3.2.1 Baseline Conditions Across Somali HEIs -----	12
3.2.2 Readiness Indicators and Staging Logic -----	19
3.2.3 Distribution of Readiness Stages Across Institutions -----	19
3.2.4 Key Gaps and Internal Variations -----	21
3.2.5 Implications for Institutions -----	22
3.3 Human Resources and Institutional Capacity -----	23
3.3.1 Baseline Conditions Across Somali HEIs -----	23
3.3.2 Readiness Indicators and Staging Logic -----	24
3.3.3 Distribution of Readiness Stages Across Institutions -----	25
3.3.4 Key Gaps and Internal Variations -----	26
3.3.5 Implications for Institutions -----	27
3.4 ICT Governance, Policy and Strategic Planning -----	28
3.4.1 Baseline Conditions Across Somali HEIs -----	29
3.4.2 Readiness Indicators and Staging Logic -----	32
3.4.3 Distribution of Readiness Stages Across Institutions -----	32
3.4.4 Key Gaps and Internal Variations -----	34
3.4.5 Implications for Institutions -----	35
3.5 Core Digital Systems Availability -----	36
3.5.1 Baseline Conditions Across Somali HEIs -----	36
3.5.2 Readiness Indicators and Staging Logic -----	39
3.5.3 Distribution of Readiness Stages Across Institutions -----	40
3.5.4 Key Gaps and Internal Variations -----	41

	3.5.5 Implications for Institutions	42
3.6	ICT Budgeting and Allocation.....	43
	3.6.1 Baseline Conditions Across Somali HEIs.....	43
	3.6.2 Readiness Indicators and Staging Logic.....	45
	3.6.3 Distribution of Readiness Stages Across Institutions.....	46
	3.6.4 Key Gaps and Internal Variations	48
	3.6.5 Implications for Institutions	49
3.7	System and Network Security	49
	3.7.1 Baseline Conditions Across Somali HEIs.....	50
	3.7.2 Readiness Indicators and Staging Logic.....	52
	3.7.3 Distribution of Readiness Stages Across Institutions.....	53
	3.7.4 Key Gaps and Internal Variations	54
	3.7.5 Implications for Institutions	55
4	National Readiness Synthesis and Typologies	57
	4.1 Aggregate Readiness Patterns Across Domains	57
	4.1.1 Cross-domain readiness distribution	57
	4.1.2 Common cross-domain mismatch patterns.....	61
	4.2 Readiness Tiers as the Primary Synthesis Lens.....	63
	4.2.1 Tier framework and interpretation	63
	4.2.2 Distribution of institutions across tiers	63
	4.2.3 What differentiates tiers nationally	64
	4.3 Typologies Within Tiers.....	65
	4.3.1 Why typologies within tiers.....	65
	4.3.2 Typology distribution within tiers	67
	4.3.3 Typologies by tier.....	68
	4.4 Structural vs Institutional Bottlenecks	70
	4.4.1 Structural bottlenecks: System-level constraints shaping readiness	70
	4.4.2 Institutional bottlenecks: Internal capacity and coherence gaps	71
	4.4.3 How can tiers and typologies be used to distinguish between different types of bottleneck?.....	71
	4.4.4 Implications for national interpretation	72
5	Regional Benchmarking: Somalia in Comparative Perspective	73
	5.1 Purpose and Scope	73
	5.2 Benchmarking Framework and Method	74
	5.3 Comparative National Readiness by Domain	75
	5.3.1 Infrastructure and connectivity	76
	5.3.2 Digital systems.....	78
	5.3.3 Human resources	79
	5.3.4 Governance and planning.....	81
	5.3.5 Financial sustainability.....	83
	5.3.6 Data security	85
6	AI and Emerging Technologies	87
	6.1 Current Awareness and Experimentation	87
	6.2 Readiness Gaps and Risks	88
	6.3 Strategic Positioning	90
7	Implications for Policy, Investment and Partnerships	91

7.1	Action Priorities	91
7.1.1	Sector-wide minimum actions	91
7.1.2	Differentiated pathways by readiness tier	92
7.1.3	Typology-sensitive targeting within tiers	94
7.2	Investment Packages and Sequencing	98
7.2.1	Package A – Foundational Infrastructure and Reliability	98
7.2.2	Package B – Shared digital services and core platforms	99
7.2.3	Package C – Institutional systems and integration	99
7.2.4	Package D – Operations, Capability and Service Management	100
7.2.5	Package E – AI-ready enablers and responsible innovation	101
7.2.6	Sequencing rules and prerequisites	105
7.3	Partnership and Delivery Models	106
7.3.1	Shared delivery models	107
7.3.2	Market-facing partnerships	108
7.3.3	Government’s enabling role and coordination mechanisms	109
7.4	Sustainability, Financing and Incentives	111
7.4.1	CapEx vs. OpEx sustainability logic	111
7.4.2	Financing and cost-sharing models	111
7.4.3	Institutional sustainability requirements	113
7.5	Implementation, accountability and the learning cycle	114
7.5.1	Implementation architecture and governance	115
7.5.2	Monitoring and evidence of progress	117
7.5.3	Risk management and safeguards	118
8	Conclusions and Way Forward	120
	Domain 1 – Infrastructure and Connectivity	131
	Domain 3: ICT Governance and Planning	134
	Domain 4: Digital Systems and Learning Technologies	135
	Domain 5: Financial Sustainability	136
	Domain 6: Data Security and Risk Management	137

List of Figures

Figure 1: Total student enrolment by institution size-----	10
Figure 2: Institutional e-readiness domains and indicator dimensions-----	11
Figure 3: Bandwidth per student by institutional size -----	12
Figure 4: Bandwidth per student by institutional size-----	15
Figure 5: Monthly connectivity cot verses contracted bandwidth -----	16
Figure 6: Wi-Fi coverage across campus -----	17
Figure 7: Distribution of readiness stages for ICT infrastructure and systems -----	20
Figure 8: Distribution of readiness stages for Human Resources and ICT Organisation -----	25
Figure 9: Distribution of readiness stages for ICT governance, policy and strategic planning -----	33
Figure 10: Distribution of readiness stages for digital systems and learning technologies ----	40
Figure 11: Distribution of readiness stages for financial sustainability-----	47
Figure 12: Distribution of readiness stages for data security and risk management -----	53
Figure 13: Cross-domain readiness distribution by domain-----	58
Figure 14: Mean domain scores across institutions-----	58
Figure 15: Distribution of scores within each domain -----	59
Figure 16: Distribution of institutions by readiness tier -----	64
Figure 17: Domain flag signatures underlying readiness typologies -----	67
Figure 18: Distribution of typologies within readiness tiers-----	67
Figure 19: Overall prevalence of readiness typologies across institutions -----	68
Figure 20: Domain flag profiles of tier 3 institutions -----	69

List of Tables

Table 1: Distribution of institutions by size category-----	9
Table 2: Distribution of student enrolment by institution size -----	10
Table 3: Distribution of institutions by institutional type -----	11
Table 4: Connectivity and reliability indicators across surveyed institutions -----	13
Table 5: Bandwidth availability relative to institutional population -----	13
Table 6: Bandwidth per student by institutional size -----	14
Table 8: Campus networking indicators. -----	17
Table 9: Computing resources supporting learning and administration -----	18
Table 10: Power and energy conditions affecting ICT operations-----	18
Table 11: ICT organisational structures and reporting lines -----	23
Table 12: ICT staffing presence and role composition -----	24
Table 13: ICT operational support practices -----	24
Table 14: ICT strategy and planning indicators-----	29
Table 15: ICT policy framework (policy presence and breadth) -----	29
Table 16: ICT policy coverage by policy type -----	30
Table 18: Monitoring, feedback and review mechanisms -----	31
Table 19: Availability of core digital systems -----	37
Table 20: System integration across institutional platforms-----	37
Table 21: Institutional usage and digitisation indicators-----	38
Table 22: Pedagogical and accessibility signals-----	39
Table 23: ICT budget structures-----	44
Table 24: ICT budget coverage and scale (institutions with a dedicated ICT budget line)-----	44
Table 25: ICT funding sources and cost recovery mechanisms (institutions with a dedicated ICT budget line) -----	45
Table 26: Financial governance and sustainability signals (institutions with a dedicated ICT budget) -----	45
Table 27: Security responsibility and awareness-----	50
Table 28: Core security and access controls -----	51

List of Abbreviations

Abbreviation	Meaning / Expansion
AI	Artificial intelligence
AUP	Acceptable Use Policy
BYOD	Bring Your Own Device
CapEx	Capital expenditure
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CSIRTs	Computer Security Incident Response Team
DLMS	Digital Library Management System
DPA	Data Protection Act
EA-RDIP	Eastern Africa Regional Digital Integration Project
ERP	Enterprise Resource Planning
FGS	Federal Government of Somalia
FMS	Federal Member States
GPU	Graphics Processing Unit
GSM	Global System for Mobile Communications
HEI	Higher Education Institution (plural: HEIs)
HPC	High Performance Computing
HR	Human Resource
HRIS	Human Resources Information System
ICT	Information and Communication Technology
ICT Policy	Information and Communication Technology Policy
IQR	Interquartile range
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
KCL	Knowledge Consulting Ltd
KENET	Kenya Education Network
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
NCHE	National Commission for Higher Education
NOC	Network Operations Centre
NREN	National Research and Education Network (plural: NRENs)
ODK	Open Data Kit
OER	open educational resources
OpEx	Operational expenditure
PIU	Project Implementation Unit

PPP	Public–Private Partnership
QA	Quality assurance
QoS	Quality of Service
RBAC	Role-based access control
RENU	Research and Education Network for Uganda
RIF	RENU Identity Federation
RwEdNet	Rwanda Education Network
SLA	Service Level Agreement
SomaliREN	Somali Research and Education Network
SOPs	Standard operating procedures
SSO	Single Sign-On
ToR	Terms of Reference
UbuntuNet	UbuntuNet Alliance for Research and Education Networking
UNESCO	United Nations Educational, Scientific and Cultural Organization
UPS	Uninterruptible Power Supply
UR	University of Rwanda
VPN	Virtual Private Network
WAN	Wide Area Network
WB	World Bank

Executive Summary

This report presents the findings of the SomaliREN Higher Education E-Readiness Assessment. This assessment establishes a baseline for digital readiness at various Somali higher education institutions (HEIs). The assessment examines the conditions that enable or constrain the reliable deployment, management, and long-term sustainability of digital technologies that support core academic and administrative functions.

The assessment does not measure individual digital skills or student access, nor does it attempt to rank universities. Instead, it evaluates the systems, infrastructure, governance, operational capacity, and financial foundations that

determine the reliability and sustainability of digital services. The findings are intended to inform policy, investment and partnership decisions at institutional and system levels, supporting a realistic, staged approach to the digital transformation of Somali higher education.

Overview of the analytical framework

The assessment targeted 55 institutions across Somali regions and received responses from 50 institutions. Data were primarily collected through a structured institutional survey administered to ICT leadership and, where necessary, other relevant institutional staff.

Institutions were assessed across six core domains:



ICT infrastructure and systems



Human resources and institutional capacity



ICT governance, policy and strategic planning



ICT budgeting and financial sustainability



Data security, privacy and risk management



Artificial intelligence (AI) and emerging technologies (exploratory)



The availability and deployment of core digital systems (including pedagogical integration)

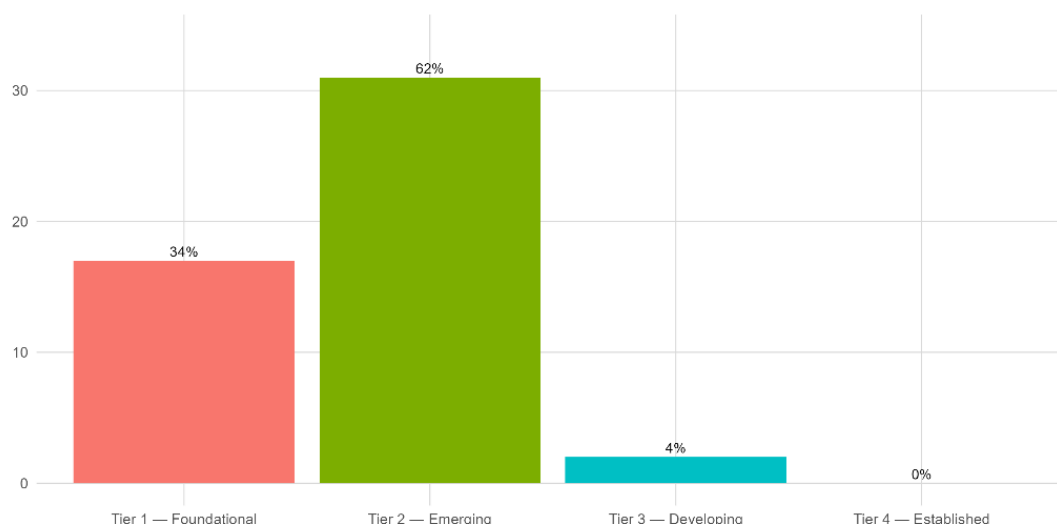
The findings were synthesised using a tiered readiness framework supported by institutional typologies. This framework is intended to be used as a staging and sequencing tool rather than as a performance scorecard. It highlights the most significant constraints and appropriate actions at each stage of readiness.

Headline findings: tier distribution and readiness reality

The assessment found that participating institutions were distributed across Tiers 1 to 3 of digital readiness, with Tier 3 representing the highest level observed in the dataset. No institution meets the full conditions associated with Tier 4. Tier

4 is therefore retained in the framework solely as an aspirational reference point aligned with regional and international good practice, rather than as an observed category.

Across all tiers, digital readiness is best characterised as uneven and fragile rather than absent. Many institutions have made tangible progress in acquiring connectivity, deploying basic systems or setting up ICT units. However, these assets often operate under conditions of constrained reliability, weak institutionalisation and limited sustainability. Power instability, single-provider connectivity, under-staffed ICT teams, undocumented systems and ad hoc financing arrangements remain commonplace.



Importantly, tier placement should not be interpreted as a judgement of institutional ambition or effort. Rather, it reflects the current configuration of constraints and the extent to which foundational conditions — reliability, operational capacity, governance and sustainable financing — have been addressed.

Typologies: explaining variation within tiers

Institutions within the same tier often have very different constraint profiles. To account for this, the assessment introduces typologies of institutions that are nested within tiers. These typologies explain why institutions at similar stages of readiness may require different intervention pathways.

A core cross-cutting finding is that institution-by-institution approaches have their limits.

A central finding of the assessment is that many of the most persistent

and costly bottlenecks facing Somali higher education institutions cannot be effectively solved on a campus-by-campus basis. These include:

- » High and volatile connectivity costs
- » Limited bargaining power with service providers
- » Duplication of infrastructure and services across institutions
- » Inconsistent security practices and exposure to shared risks
- » Dependence on short-term project funding without sustainable cost-sharing models.

While institution-level reforms remain necessary, the assessment concludes that system-level coordination and shared delivery mechanisms are essential for achieving long-term improvements in reliability, affordability and service quality.

SomaliREN is a system-level delivery platform

International experience shows that peer countries have improved higher education connectivity and digital services by establishing strong National Research and Education Networks (NRENs), rather than through isolated campus investments. These NRENs aggregate demand, coordinate procurement and provide shared services. The assessment concludes that Somalia could follow a similar trajectory by strengthening the role of SomaliREN as a system-level delivery platform, expanding participation, pooling connectivity procurement and scaling up shared services and support capacity. Beyond providing connectivity, SomaliREN can facilitate collective solutions for bandwidth procurement and resilience, shared platforms (e.g. authentication, learning, and digital library services), and coordinated approaches to cybersecurity, risk management, and institutional support. Therefore, strengthening SomaliREN's participation and service delivery capacity is a structural requirement for addressing system-wide bottlenecks in a cost-effective and sustainable manner.

Time-bound opportunity: EARDIP as a catalytic platform

The assessment identifies the Eastern Africa Regional Digital Integration Project (EARDIP) as a time-bound opportunity to catalyse system-level change. Instead of financing fragmented campus upgrades, EARDIP can be used to establish shared foundations through SomaliREN, accelerating early onboarding into pooled connectivity arrangements and supporting the development of shared services. This will also put sustainable cost-sharing, accountability and coordination mechanisms in place across government, SomaliREN, institutions and market providers. Without robust system-level design, EARDIP investments risk perpetuating fragmentation and short-termism. However, when aligned with clear sequencing and governance, these investments can facilitate a transition from project-driven upgrades to managed, sustainable service delivery.

Investment packages and sequencing logic

In order to translate the findings into actionable guidance, the assessment groups the interventions into five investment packages (A–E), which have clear dependencies. The sequencing emphasises the prioritisation of foundational reliability and service management at an early stage, the pursuit of core systems where adoption capacity exists, the scaling of security once governance and controls are in place, and the deferral of advanced capabilities until the foundations are stable. This staged approach aims to reduce fragmentation, improve absorptive capacity and safeguard long-term sustainability.

Distinguishing between system-level and institution-level actions

The assessment clearly distinguishes between the two, as they involve different actors and levels of accountability.

System-level actions include:

- » Establishing pooled procurement and shared service frameworks through SomaliREN
- » Setting baseline standards and interoperability requirements
- » Creating enabling procurement and financing mechanisms
- » Coordinating donor and project investments around shared priorities
- » Supporting learning cycles, benchmarking and peer exchange.

These actions primarily involve the Ministry of Communications and Technology (MoCT), the Ministry of Education, Culture and Higher Education (MoECHE), the National Council for Higher Education (NCHE), SomaliREN, and development partners. They are essential for reducing structural costs and risks.

Institution-level actions include:

- » Strengthening ICT governance and strategic planning
- » Clarifying the roles and responsibilities of ICT units
- » Improving documentation, maintenance, and service management
- » Building staff capacity and retention mechanisms
- » Preparing institutions to adopt and use shared services effectively.

While institutions are not expected to resolve system-level constraints independently, they do play a critical role in ensuring that shared investments are effectively absorbed and sustained.

Implementation, governance and accountability

To support effective implementation, the assessment proposes a lightweight yet disciplined implementation architecture comprising:

- » A strategic steering function for policy alignment
- » Technical working groups for design and coordination
- » Delivery entities responsible for execution
- » A dedicated PMO or secretariat function to coordinate timelines, procurement, reporting and risk management.

Monitoring should rely on a small set of “signal indicators” that track service reliability, uptake and sustainability rather than complex reporting burdens. Risk management measures should emphasise clarity of roles, realistic sequencing and the avoidance of undefined or unenforceable metrics.

Strategic direction and key messages

The findings point to a clear strategic direction. Somalia’s higher education sector has made meaningful progress, but further improvements depend on shifting from fragmented, institution-by-institution approaches to a coordinated, system-wide delivery model.

Leveraging SomaliREN as a delivery platform and using EARDIP as a catalytic opportunity can enable stakeholders to convert existing assets into reliable, sustainable services and lay the foundations for inclusive digital transformation across the sector.

1 Introduction and Context

1.1 Digital Transformation and Higher Education in Fragile Contexts

Digital transformation has become an important driver of reform in higher education systems across low- and middle-income countries. Digital technologies provide universities with new ways to increase access, enhance teaching and learning quality, strengthen institutional management and connect to regional and global knowledge networks. In contexts where resources are limited and institutional systems are still developing, progress in digital transformation relies more on establishing sustainable institutional foundations over time than on rapid technology adoption.

In Somalia, for example, recent developments in the telecommunications sector, including the expansion of mobile broadband and the landing of multiple submarine cables, have improved the country's overall connectivity potential and created new opportunities for digital service delivery. However, the effective integration of digital technologies within higher education institutions remains uneven. Many universities continue to operate with limited ICT infrastructure, fragmented digital systems and limited institutional capacity to plan, manage and sustain digital investments.

Higher education institutions play a critical role in Somalia's broader development and digital ambitions. As centres for human capital development, research and professional training, they are central to building the skills needed for public administration, private sector growth and participation in the digital economy. They also serve as anchor institutions for advanced connectivity and digital services. As a result, weaknesses in institutional digital readiness, whether related to infrastructure, systems, governance or

human capacity, have implications that extend beyond individual institutions to the wider national development agenda.

The digital environment within Somali universities is shaped by a combination of technical, organisational and financial constraints. ICT infrastructure and campus networks are often limited in scale and reliability, and core digital systems, such as learning and student information management systems, are unevenly deployed and not always well integrated. Shortages of specialised ICT staff, evolving governance arrangements for ICT decision-making and limited predictability in funding for digital infrastructure and services compound these challenges.

Experience from comparable contexts shows that successful digital transformation in higher education requires more than connectivity alone. Sustainable progress depends on infrastructure investments being aligned with institutional capacity, clear governance structures and realistic financial planning. Without these elements, digital systems risk remaining underutilised or difficult to maintain, and vulnerable to operational and security risks. This emphasis on sequencing and enabling conditions is consistent with World Bank guidance, which advises against technology-first approaches and emphasises the pivotal role of institutional preparedness in ensuring the meaningful and lasting impact of digital investments.¹

Against this backdrop, it is essential to establish a clear and evidence-based understanding of the current state of digital readiness across Somali higher education institutions. A structured institutional e-readiness assessment provides a practical baseline for identifying priority areas for improvement, planning interventions and ensuring that future investments in digital infrastructure

1 World Bank (2024). Digital Pathways for Education: Enabling Greater Impact for All, <https://www.worldbank.org/en/topic/edutech/publication/digital-pathways-education-enabling-learning-impact>

and capacity development are aligned with institutional realities and long-term sustainability considerations.

1.2 Objectives and Scope

Based on the contextual considerations outlined above, this assessment aims to establish a clear and systematic understanding of the current level of digital readiness at selected higher education institutions in Somalia. Specifically, it evaluates institutional readiness for digital transformation, focusing on the capabilities, systems and conditions that are necessary for universities to deploy, manage and maintain digital technologies effectively in support of teaching, learning, research and administration.

The assessment is explicitly **institutional in scope**. It examines the readiness of higher education institutions as organisations, rather than the digital skills or competencies of individual students or academic staff. Although individual digital literacy and pedagogical practices are important elements of digital transformation, they are influenced by—and dependent on—broader institutional factors, such as infrastructure availability, system integration, governance arrangements, staffing capacity and financial sustainability. The assessment therefore prioritises these institutional foundations as the primary determinants of sustainable digital transformation.

To this end, the assessment examines institutional readiness across a defined set of core domains reflecting international good practice and regional experience, while remaining relevant to the Somali higher education context. These domains include the availability and quality of ICT infrastructure and systems, the human resources and organisational capacity needed to support ICT operations, governance and policy arrangements, strategic planning, the availability and integration of core digital academic and administrative systems, the adequacy

and predictability of ICT budgeting and resource allocation, and institutional approaches to system and network security. Additionally, the assessment incorporates an exploratory module on artificial intelligence and emerging technologies, focusing on initial awareness and experimentation rather than established deployment.

The scope of the assessment has been deliberately defined to avoid overextension or duplication with other initiatives. The assessment does not evaluate individual digital skills, learning outcomes or pedagogical effectiveness at the classroom level. Nor does it assess student access to personal devices or connectivity outside the institutional environment or provide a detailed audit of curricular content or research outputs. While these areas are important, they require different methodological approaches and are beyond the intended scope of an institutional e-readiness diagnostic.

By maintaining a clear focus on institutional readiness, the assessment provides a practical, policy-relevant baseline to inform institutional planning, sector-level coordination and future investment decisions. The resulting evidence is intended to support a phased and realistic approach to digital transformation in Somali higher education that is aligned with institutional capacities and national development priorities.

1.3 Conceptual and Analytical Framework

This assessment is based on well-established international and regional approaches to institutional e-readiness and digital transformation in higher education. It has been deliberately adapted to reflect the maturity level and operational realities of the Somali higher education sector. Drawing on proven frameworks and diagnostic practices, the assessment avoids replicating models designed for more mature systems.

At the regional level, the assessment builds on the experience of institutional e-readiness surveys conducted by national research and education networks, particularly those led by the Kenya Education Network Trust (KENET).² These surveys demonstrate the value of diagnostics focused on institutions that examine not only connectivity, but also campus networks, digital systems, governance arrangements and organisational capacity. The present assessment adopts this institutional focus and the concept of staged readiness, applying indicators and analytical approaches that are appropriate to Somalia's current context.

The assessment is also informed by UNESCO's work on digital transformation in higher education, which emphasises aligning infrastructure, human capacity, governance, financial planning and academic systems to support sustainable transformation.^{3,4,5} This holistic perspective is reflected in the multi-domain structure of the assessment and its focus on institutional enablers rather than isolated technologies.

In addition, the assessment aligns with the World Bank's approach to institutional diagnostics, which prioritises evidence-based baselines, realism about capacity constraints, and the use of diagnostics to inform phased and sequenced investments.^{6,7} In line with this approach, the assessment is intended to facilitate policy discussions and investment planning within initiatives such as the Eastern Africa Regional Digital Integration Project (EA-RDIP), rather than producing rankings or offering prescriptive solutions.

Although based on these well-established approaches, the assessment has been adapted to the Somali higher education environment. The indicators and analytical methods reflect the varying levels of institutional maturity, the evolving governance structures and the practical resource constraints. This ensures the findings are credible and interpretable for institutional leaders, government authorities and development partners.

2 <https://ereadiness.kenet.or.ke/>

3 UNESCO (2023) – Global Education Monitoring Report: Technology in Education, <https://doi.org/10.54676/UZQV8501>

4 UNESCO-ICHEI (2022) – Digital Transformation of Higher Education Teaching and Learning, <https://en.ichei.org/Uploads/Download/2022-05-16/62820a2a9bceb.pdf>

5 UNESCO (2025) – Report on Digital Transformation in Higher Education in South Asia, <https://unesdoc.unesco.org/ark:/48223/pf0000394970>

6 World Bank (2021) – Digital Transformation of Education Systems: Insights from the EdTech Readiness Index (ETRI), <https://www.worldbank.org/en/topic/education/brief/edtech-readiness-index>

7 World Bank (2018) – World Development Report 2018: Learning to Realize Education's Promise. <https://openknowledge.worldbank.org/bitstream/handle/10986/28340/9781464810961.pdf>

1.4 Structure of the Report

This report is structured to guide the reader from the context and methodology, through institution-level evidence across the six e-readiness domains, to synthesis, benchmarking, and actionable recommendations. It includes:

- 01 Chapter 1** introduces the assessment context, objectives and scope, as well as the conceptual and analytical framework that underpins the study.
- 02 Chapter 2** describes the methodology and assessment framework, including institutional coverage, data management and limitations, the logic of readiness staging and the approach to benchmarking.
- 03 Chapter 3** profiles the participating institutions and describes institutional groupings and baseline digital environment characteristics.
- 04 Chapter 4** presents the core findings by e-readiness domain using a consistent structure for each domain.
- 05 Chapter 5** synthesises national readiness patterns across domains using readiness tiers as the primary lens, introducing typologies within tiers to explain common mismatch patterns and differentiate between structural and institutional bottlenecks.
- 06 Chapter 6** provides regional benchmarking, positioning Somalia in a comparative context by domain and clarifying the benchmarking framework and method used.
- 07 Chapter 7** examines AI and emerging technologies, focusing on current awareness, readiness gaps, risks and strategic positioning.
- 08 Chapter 8** translates the findings into implications for policy, investment and partnerships, including a phased investment pathway for implementation planning.
- 09 Chapter 9** concludes with a summary of the overall approach and key next steps.

The appendices provide supporting detail: Appendix A contains the survey instrument; Appendix B defines the indicators by domain and Appendix C lists the benchmark sources used in Chapter 6.

2 Methodology and Assessment Framework

This chapter outlines the methodology employed to evaluate the digital readiness of selected higher education institutions in Somalia. It describes the design of the assessment framework and tool, as well as the analytical logic behind the findings presented in subsequent chapters.

2.1 Assessment Design and Framework

The institutional e-readiness assessment is a structured diagnostic tool designed to evaluate higher education institutions' capacity to deploy, manage and sustain digital technologies in support of their academic and administrative functions. Rather than focusing on individual digital skills or classroom-level practices, the assessment focuses on institutional systems, capabilities and enabling conditions.

The assessment framework is organised around six core domains that reflect international best practice and regional experience while remaining relevant to Somali higher education. These domains address:

- » ICT infrastructure and systems
- » Human resources and institutional capacity
- » ICT governance, policy and strategic planning
- » Availability and integration of core digital academic and administrative systems
- » ICT budgeting and resource allocation
- » system and network security.

In addition, an exploratory domain on artificial intelligence (AI) and emerging technologies has been included to capture initial awareness and experimentation, without assuming mature deployment.

Within each domain, the assessment uses a set of indicators designed to capture three complementary dimensions of institutional readiness: the existence of key systems, policies or structures; the capacity to operate and support them effectively; and the extent to which they are integrated into institutional practices. This structure enables the assessment to move beyond binary measures of availability, providing a more nuanced picture of institutional readiness.

The assessment is explicitly diagnostic in nature. It is not intended to be an audit, a compliance exercise or a ranking of institutions. Instead, it is designed to establish a baseline for comparative analysis, identify common gaps and constraints, and inform phased planning and investment decisions at institutional and sector levels. To this end, the framework takes a readiness-stage approach, recognising that digital transformation is a progressive process in which institutions may be at different stages in different areas.

The assessment framework draws on established approaches used in regional institutional e-readiness surveys and international digital transformation frameworks. However, it has been adapted to reflect the varying levels of maturity, resource constraints and operational realities of Somali higher education institutions.

2.2 Data Collection and Institutional Coverage

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. Based on enrolment-based groupings derived from the observed distribution of reported student populations, **17 HEIs** (34%) are categorised as **small** (with fewer than 1,000 students), **21 HEIs** (42%) as **medium** (with 1,000–3,999 students), and **12 HEIs** (24%) as **large** (with 4,000 or more students). 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.

Data were primarily collected through a structured institutional survey administered to ICT directors or designated ICT units, who were selected based on their responsibility for digital infrastructure, systems, and services. Where ICT functions were distributed across departments, responses were supplemented by contributions from staff involved in academic administration, finance or institutional management, ensuring adequate coverage of institutional digital operations.

The data collection process combined self-administered online surveys with targeted follow-up and clarification to resolve ambiguities and improve the completeness of the responses. Minor refinements were made to the survey instrument during implementation to improve clarity and applicability. These refinements did not affect the underlying assessment framework or indicators, and responses across survey versions were analysed together.

Participation and response completeness varied across assessment domains, reflecting differences in institutional capacity and information availability. The analysis therefore emphasises sector-level patterns and institutional groupings rather than exhaustive institution-level profiling. This approach enables robust comparative analysis while accurately reflecting data constraints across the higher education sector.

2.3 Data Management, Quality Assurance and Limitations

The survey responses were compiled into a consolidated dataset, which was then subjected to systematic data cleaning and harmonisation prior to analysis. This involved standardising variable names and response categories across survey versions, resolving obvious inconsistencies and ensuring consistent interpretation of indicators across institutions. Where questions were added or removed during the refinement of the questionnaire, the corresponding variables were transparently retained or omitted, and missing values were treated as structural rather than respondent error.

Quality assurance measures focused on internal consistency and plausibility rather than external verification. Responses were reviewed to identify incomplete records, contradictory answers and values that fell outside the expected range. Where necessary, follow-up clarifications were undertaken with institutional respondents to resolve ambiguities. Given the institutional focus of the assessment, responses were evaluated for coherence at the domain level rather than on the basis of individual items alone.

The analysis acknowledges that the assessment is primarily based on institutional self-reporting. Although the respondents were selected for their operational responsibility and familiarity with institutional ICT systems, the availability and accuracy of the information provided varied across institutions and domains. Consequently, the findings should be interpreted as indicative of institutional readiness patterns and stages rather than as precise measurements of system performance or utilisation.

Several contextual and methodological limitations should therefore be noted. For example, data coverage is uneven across domains, reflecting differences in institutional maturity and record-keeping practices. The assessment does not include independent technical audits or on-site

verification of infrastructure and systems. Additionally, the evolving operational environment and the resource constraints faced by many institutions may impact the timeliness and completeness of the reported information.

However, these limitations do not undermine the assessment's usefulness as an institutional diagnostic tool. Rather, they emphasise the importance of interpreting the findings in a comparative and directional manner. The assessment is intended to inform the prioritisation and sequencing of interventions in strategic planning, rather than to serve as a compliance tool or definitive evaluation of institutional performance.

2.4 Analytical Approach and Readiness Staging

The analysis uses a two-tiered approach, balancing descriptive clarity with structured interpretation. The **first layer establishes an institutional baseline** by analysing survey responses at the indicator and domain levels, describing the current state of digital readiness across participating higher education institutions. This descriptive analysis focuses on the presence, distribution and characteristics of infrastructure, systems, governance arrangements, capacity and resources without any aggregation or scoring. It provides an empirical basis for understanding how digital technologies are currently deployed and managed within institutions.

The **second layer introduces a readiness staging approach** to support comparative analysis and synthesis across institutions and domains. Readiness staging characterises institutional maturity in a structured yet non-deterministic manner, recognising that digital transformation is a progressive process rather than a binary condition. Institutions may occupy different readiness stages in different domains, reflecting uneven development and context-specific constraints.

For each domain, indicators were interpreted collectively to characterise institutional conditions along a small number of readiness stages, ranging from early or nascent conditions to more established and institutionalised arrangements. These stages are qualitative, informed by patterns observed across multiple indicators rather than mechanical scoring or weighted indices. The staging process prioritises internal coherence and plausibility, ensuring that assigned stages reflect consistent institutional conditions rather than isolated responses.

Aggregation is applied cautiously and transparently. Rather than producing composite scores or rankings, domain-level readiness stages are used to identify distributions and common patterns across institutions. At the synthesis stage, cross-domain comparisons highlight systemic strengths and recurring gaps, as well as interdependencies between domains. For example, the relationship between infrastructure availability, human capacity, governance arrangements and financial sustainability is examined.

This quantitative-light approach avoids constructing composite indices or league tables, as these can obscure institutional realities and imply false precision, particularly in contexts with heterogeneous capacity and uneven data availability. Instead, the readiness staging framework provides a shared analytical language that supports interpretation, benchmarking and policy dialogue while remaining accessible to institutional leaders and policymakers.

The readiness staging framework underpins the organisation and interpretation of findings in Chapters 4 and 5 and informs the national-level comparison presented in Chapter 6. By emphasising progression and variability rather than static assessment, the analytical approach facilitates forward-looking discussions on sequencing, prioritisation and pathways for institutional and sector-level digital transformation.

2.5 Benchmarking Approach

This assessment uses benchmarking to place the digital readiness of Somali higher education institutions within a broader regional context. Benchmarking does not seek to rank institutions or countries, but rather to provide directional comparisons that support the interpretation of findings and inform policy dialogue, investment prioritisation and sequencing.

This approach focuses on national-level comparisons across selected readiness domains, drawing on publicly available studies, institutional e-readiness surveys and sector analyses from comparator countries in the region – specifically Kenya, Uganda and Rwanda. These countries were selected based on the availability of relevant evidence on the digital readiness of higher education institutions, the presence of well-established national research and education network (NREN) ecosystems, and their status as relevant regional peers.

A quantitative-light framework is used for comparative analysis, aligning Somalia's aggregated institutional findings with indicative readiness stages observed in comparator countries. This approach relies on the qualitative interpretation of documented institutional practices, system deployment patterns and governance arrangements rather than

harmonised numerical indicators or composite indices. Differences in data sources, methodologies and sector maturity are therefore explicitly acknowledged, and comparisons are presented as indicative rather than definitive.

Benchmarking is applied selectively to core domains where regional reference information is sufficiently robust to support meaningful comparisons. Areas characterised by early experimentation or high contextual variability, such as artificial intelligence and emerging technologies, are excluded from benchmarking in order to avoid false equivalence.

The benchmarking approach outlined here informs the comparative analysis presented in Chapter 6. The assessment ensures that benchmarking enhances interpretation without overstating precision or obscuring institutional realities by maintaining a clear separation between methodological framing and analytical results.

3 Findings by E-Readiness Domain

This chapter presents the findings of the institutional e-readiness assessment, based on data collected from participating higher education institutions in Somalia. It examines the conditions within institutions that facilitate the deployment, management and long-term sustainability of digital technologies in support of teaching, learning, research and administration.

The analysis is organised by thematic domain and is based on a descriptive baseline assessment of institutional conditions. Rather than relying on composite indices, the chapter identifies patterns, gaps and interdependencies across institutions, recognising that digital readiness is multidimensional and uneven across functional areas.

3.1 Profile of Participating Institutions

Before examining institutional readiness in specific areas, this section provides profiles of the participating institutions to establish the structural context in which digital systems are planned, deployed and managed. The scale and complexity of digital operating environments are shaped by institutional size, student enrolment patterns and ownership type, and are therefore critical for interpreting the findings presented in subsequent sections.

Drawing on three core dimensions — institutional size, distribution of student enrolment, and institutional type — this section describes the composition of the assessed institutions and highlights structural factors that influence digital readiness across the system.

3.1.1 Distribution of institutions by size

Participating institutions were classified into three size categories based on total student enrolment:

- » Small institutions (fewer than 1,000 students)
- » Medium institutions (1,000–3,999 students)
- » Large institutions (4,000 students or more)

These thresholds were derived empirically from the observed enrolment distribution across participating institutions and reflect natural clustering in institutional scale.

Table 1: Distribution of institutions by size category

Size of institution	Number of institutions	Proportion (%)
Small (< 1,000)	17	34
Medium (1,000 – 3,999)	21	42
Large (≥ 4,000)	12	24

Table 1 highlights the predominance of small and medium-sized institutions within the Somali higher education landscape, alongside a smaller group of larger institutions operating at a significantly greater scale.

3.1.2 Distribution of student enrolment by institutional size

Although small and medium-sized institutions together account for over three-quarters of participating institutions, student enrolment is highly concentrated within a smaller number of large institutions. This section summarises the distribution of total student enrolment across size categories.

Despite representing one-third of the sample, small institutions account for only 8,811 students, equivalent to 6.7% of the total enrolment captured by the assessment. Medium-sized institutions enrol 49,259 students, representing 37.3% of the total. By contrast, large institutions – just under a quarter of participating institutions – account for 74,118 students, representing 56.1% of the total student population.

Table 2: Distribution of student enrolment by institution size

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

Figure 1 illustrates this concentration visually. The disparity between the number of institutions and their share of enrolment highlights the structural importance of large institutions within the higher education system. These institutions typically operate more complex digital environments, face greater demands on infrastructure and systems, and serve a disproportionately large share of students.

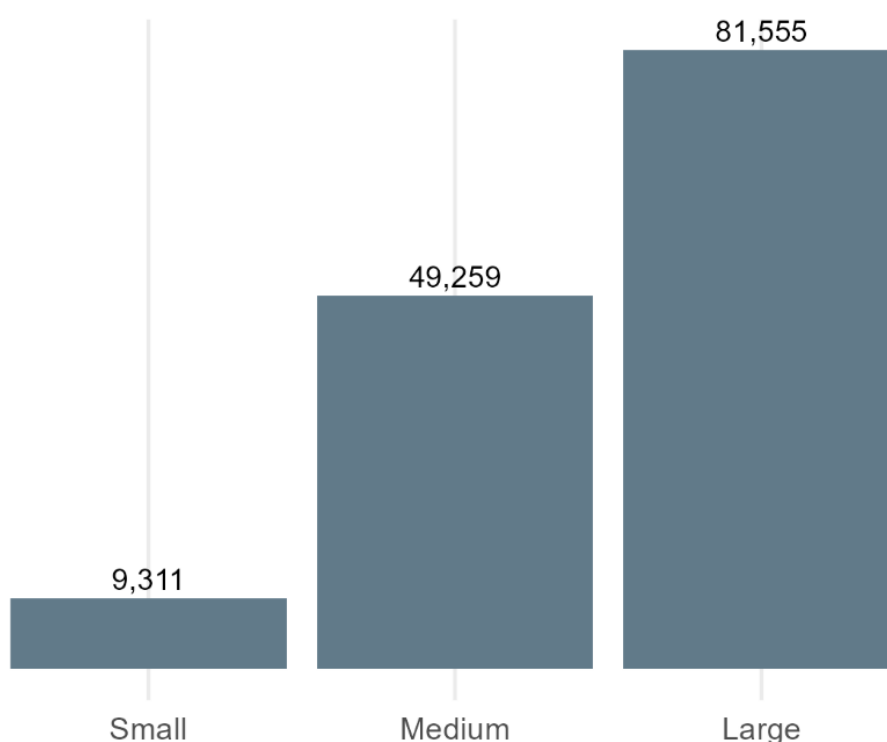


Figure 1: Total student enrolment by institution size

3.1.3 Institutional type

The assessment includes institutions that operate under various ownership and governance structures. Table 3 shows how

participating institutions are distributed across different institutional types, as reported in the survey.

Table 3: Distribution of institutions by institutional type

Type of institution	Number of institutions	Proportion (%)
Public	8	16
Private	25	50
Public–Private Partnership (PPP)	1	2
Community-owned/Foundation	15	30
Other	1	2

The majority of participating institutions fall within two dominant categories, which together account for nearly 80% of the sample. 25 institutions (50%) are private institutions, while 15 institutions (30%) are community-owned/foundation institutions. A smaller number of institutions are classified under additional types. Differences in institutional type are important when interpreting later findings, particularly with regard to governance arrangements, funding models and decision-making autonomy. All of these factors influence how digital infrastructure and systems are planned, financed and managed.

Shaded cells (grey) indicate the primary indicator dimensions examined within each domain.

	Availability and Coverage	Capacity and Skills	Governance and Planning	Integration and Usage	Sustainability and Risk
Infrastructure and Systems					
Human Resource and Institutional Capacity					
Governance Policy and Strategic Planning					
Core Digital Systems Availability					
ICT Budgeting and Allocation					
Systems and Network Security					
AI and Emerging Technologies (Exploratory)					

Figure 2: Institutional e-readiness domains and indicator dimensions

Against this institutional backdrop, the remainder of the chapter examines e-readiness across six core domains: ICT infrastructure and systems; human resources and institutional capacity; ICT governance, policy, and strategic planning; the availability of core digital systems; ICT budgeting and allocation; and system and network security. An additional exploratory domain looks at emerging practices relating to artificial intelligence and advanced digital technologies.

Each domain is analysed using a consistent analytical framework combining descriptive baseline analysis with readiness staging. Although some indicator dimensions are common to all domains — such as availability and coverage, institutional capacity, governance and planning, and system integration and sustainability — the emphasis placed on them varies depending on the nature of each domain. Figure 2 summarises the analytical framework and indicator dimensions used to structure the findings presented in Sections 3.2 to 3.7.

3.2 ICT Infrastructure and Systems

This domain evaluates the availability, quality and reliability of the ICT infrastructure that supports academic and administrative activities in higher education institutions. The focus is on institutional connectivity, campus networks, computing resources and the power supply as the fundamental enablers of digital systems and services.

The assessment looks at institutional internet access, examining connectivity status, access technologies, contracted and effective bandwidth, service costs, reliability and monitoring tool usage for network performance management. These indicators capture both connectivity access and the institutional capacity to oversee and optimise its use.

Campus networking is evaluated based on the presence and coverage of local area networks, backbone technologies, on-campus fibre deployment, and the extent of wired and wireless network coverage across academic and administrative

buildings. These elements are critical to the operation of shared digital platforms and internal information systems.

The domain also evaluates institution-owned computing resources, such as computer laboratories, devices used for teaching and learning, library services and administrative systems. Attention is given to the operational status of equipment and its suitability for current software and platforms.

Finally, the assessment considers the reliability of the power supply for ICT operations, including primary energy sources, the frequency of power interruptions, the availability of backup power solutions and the use of renewable or alternative energy sources, where applicable. A stable and resilient power supply is considered an integral part of ICT infrastructure readiness.

3.2.1 Baseline Conditions Across Somali HEIs

All surveyed institutions reported having an internet connection, indicating near-universal basic connectivity at the institutional level. However, deeper indicators relating to monitoring, internal distribution, power reliability and bandwidth relative to institutional size reveal uneven infrastructure maturity and significant variability in service quality across the higher education system. Evidence suggests that, although external connectivity is largely in place, internal campus networks and operational resilience remain constraints on the reliable delivery of digital services.

Connectivity and reliability

At a high level, **all surveyed institutions report having an active internet connection**, confirming that basic external connectivity is no longer the primary barrier for Somali higher education institutions. However, **only 28% report having internet monitoring mechanisms in place**, indicating limited institutional visibility into network performance, outages or quality of service. This gap constrains institutions' ability to diagnose problems, manage vendor performance or plan capacity upgrades systematically.

Table 4: Connectivity and reliability indicators across surveyed institutions

Indicator	Summary
Institutions connected to the internet	100%
Internet monitoring in place	28%
Weekly internet downtime (median)	1 hours
Weekly internet downtime (IQR)	2 hours

Reported internet reliability varies. The median weekly internet downtime is 1 hour, with an interquartile range (IQR) of 2 hours. This suggests that, while many institutions experience relatively limited disruption, a significant proportion face more frequent or prolonged outages.

The distribution shows a small number of outliers reporting substantially higher downtime, which pulls the upper range upwards and indicates uneven reliability conditions across the system.

Internet access technologies

Institutions rely on a variety of access technologies, with fibre-based connectivity predominating, although legacy and wireless alternatives are still in use. Fibre optic connections are used by around 76% of institutions, reflecting significant progress in the availability of backbone and metro connectivity. Meanwhile, ADSL/DSL (28%) and microwave radio links (15%) remain in use, and satellite-based connections (VSAT/Starlink) are used by only a few institutions.

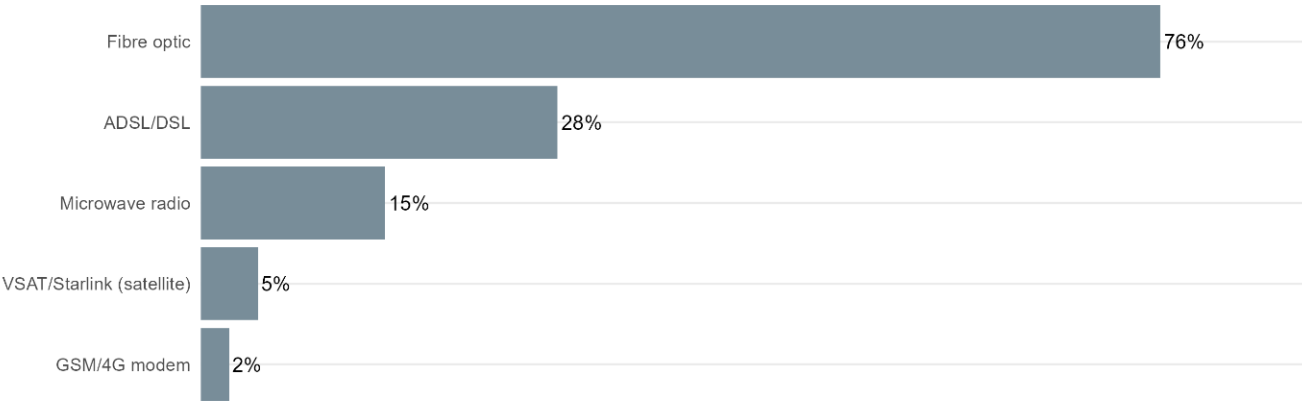


Figure 3: Internet access technologies reported by institutions

This variety of technologies suggests that, although high-capacity connectivity is becoming more widely available, redundancy and last-mile constraints persist in certain areas, particularly outside major urban centres or where fibre access is limited. A small proportion of institutions continue to rely on lower-capacity or more variable technologies, which may explain the higher levels of downtime observed at the upper end of the distribution.

Bandwidth relative to institutional size

Table 5: Bandwidth availability relative to institutional population

Indicator	Summary
Total number of institutional users (students + staff)	2069 (IQR 3306.25)
Total contracted internet bandwidth	77.5 Mbps (IQR 69)
Bandwidth available per institutional user	0.04 Mbps per user (IQR 0.066)

Although headline indicators suggest that all surveyed institutions have an internet connection, the availability of bandwidth relative to institutional size reveals a much more constrained picture. As shown in Table 5, the median institution serves 2,069 users (students and staff combined), with substantial variation in enrolment levels (interquartile range (IQR) 3,306.25). The median contracted internet capacity is 77.5 Mbps (IQR 69 Mbps), which equates to only 0.04 Mbps per user (IQR 0.066) when averaged across institutional populations. In other words, this equates to around **40 Mbps per 1,000 users** — a level that is insufficient for contemporary higher education environments, which are becoming increasingly dependent on cloud services, digital libraries, learning management systems, video conferencing and online research tools.

When considered in a comparative context, this level of provision falls short of regional practice and international guidance. For instance, Kenyan universities reported an average of **52 Mbps per 1,000 users** during the 2022–23 academic year, while the sector’s stated target was **100 Mbps per 1,000 users** to ensure adequate, high-speed access.⁸ Similarly, 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**.⁹ By contrast, the median Somali institution operates at a substantially lower level of effective bandwidth per user.

Table 6: Bandwidth per student by institutional size

Institution size category	Number of institutions	Bandwidth per student (kbps)
Small (< 1,000 students)	17	107.9 (IQR 63 – 333.3)
Medium (1,000 to 3,999)	21	35 (IQR 20 – 42.9)
Large (≥ 4,000)	12	23.1 (IQR 9.9 – 49)

Adjusting bandwidth availability for institutional scale reveals a significant and consistent “scale penalty”. As shown in Table 6, small institutions (with fewer than 1,000 students) report a median of **107.9 kbps per student**. This is compared to **35.0 kbps per student** for medium-sized institutions (with 1,000–3,999 students) and just **23.1 kbps per student** for large institutions (with 4,000 students or more). In practical terms, this implies that a medium-sized institution typically operates with the equivalent of **35 Mbps per 1,000 students**, whereas a large institution operates with around **23 Mbps per 1,000 students**. Even allowing for differences in usage patterns, these levels fall well below conservative reference benchmarks, suggesting that increases in total contracted bandwidth have not kept pace with enrolment growth.

8 https://ereadiness.kenet.or.ke/sites/default/files/ctools/2022/Annual_Core_Data_Survey_Report_2022_2023.pdf

9 <https://kcl.co.ug/wp-content/uploads/2023/01/Circulation-Version-Breaking-the-Final-Connectivity-Barriers-for-Higher-Education-Institutions-in-Africa.pdf>

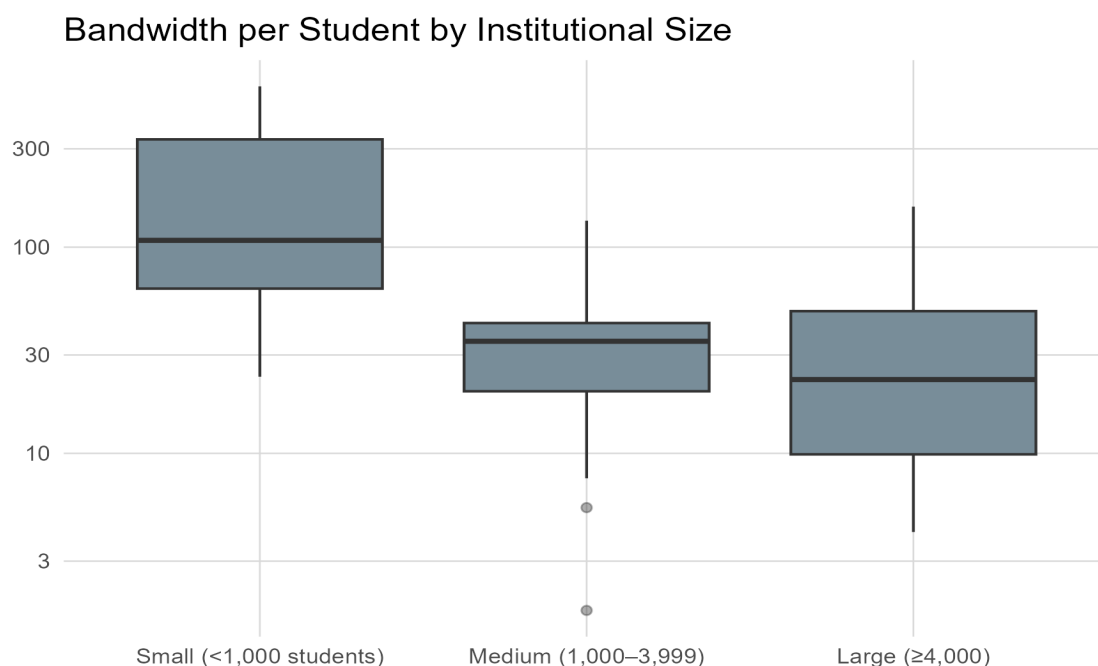


Figure 4: Bandwidth per student by institutional size

Figure 4 illustrates this pattern, showing the distribution of bandwidth per student across institutional size categories. Not only does the figure demonstrate declining median values as institutional size increases, but it also shows widening dispersion among medium and large institutions.

This suggests that the provision of bandwidth among larger campuses is

uneven and often ad hoc, with some institutions operating at extremely constrained levels. Using a logarithmic scale further highlights the magnitude of the difference between small institutions and their medium- and large-sized counterparts, thereby reinforcing the importance of size-adjusted analysis when interpreting connectivity indicators.

Table 7: Bandwidth adequacy bands by institutional size

Institution size category	Adequacy band	Institutions	Share
Small (<1,000 students)	<50 kbps (Severely constrained)	2	12%
Small (<1,000 students)	50 - 199 kbps (Constrained)	10	59%
Small (<1,000 students)	≥200 kbps (Relatively adequate)	5	29%
Medium (1,000 - 3,999)	<50 kbps (Severely constrained)	18	86%
Medium (1,000 - 3,999)	50 - 199 kbps (Constrained)	3	14%
Large (≥4,000)	<50 kbps (Severely constrained)	9	75%
Large (≥4,000)	50 - 199 kbps (Constrained)	3	25%

An adequacy-based interpretation provides a clearer picture. As summarised

in Table 7, 86% of medium-sized institutions and 75% of large institutions have a speed of **less than 50 kbps per student**. This level is classified as “severely constrained”. At these levels, institutions are likely to experience persistent congestion during peak usage periods, which limits the effective use of bandwidth-intensive applications such as synchronous online teaching, video conferencing, access to large digital research repositories and cloud-based academic services. While small institutions perform relatively better, only 29% reach levels above 200 kbps per student. This indicates that, even among smaller campuses, bandwidth adequacy remains the exception rather than the norm.

Connectivity cost pressure and procurement efficiency

In addition to bandwidth constraints, institutions face significant and inconsistent cost pressures when securing internet connectivity.

Of the 50 institutions that reported their monthly connectivity expenditure, the median cost was \$315 per month, with an average cost of \$991 and a wide interquartile range of \$1,521, which indicates highly dispersed spending levels across institutions. When costs are normalised by contracted bandwidth, the median cost is \$5.13 per Mbps, with an interquartile range of 15.7 and observed values ranging from 0.3 to 73.3 per Mbps.

As Figure 5 illustrates, plotting monthly connectivity cost against total contracted bandwidth reveals no consistent relationship between higher expenditure and greater capacity. Some institutions incur relatively high monthly costs for modest bandwidth, while others obtain substantially larger capacity at a comparable or lower cost. This dispersion suggests marked differences in procurement arrangements, provider pricing and economies of scale, rather than systematic variation driven by institutional size or bandwidth demand alone.

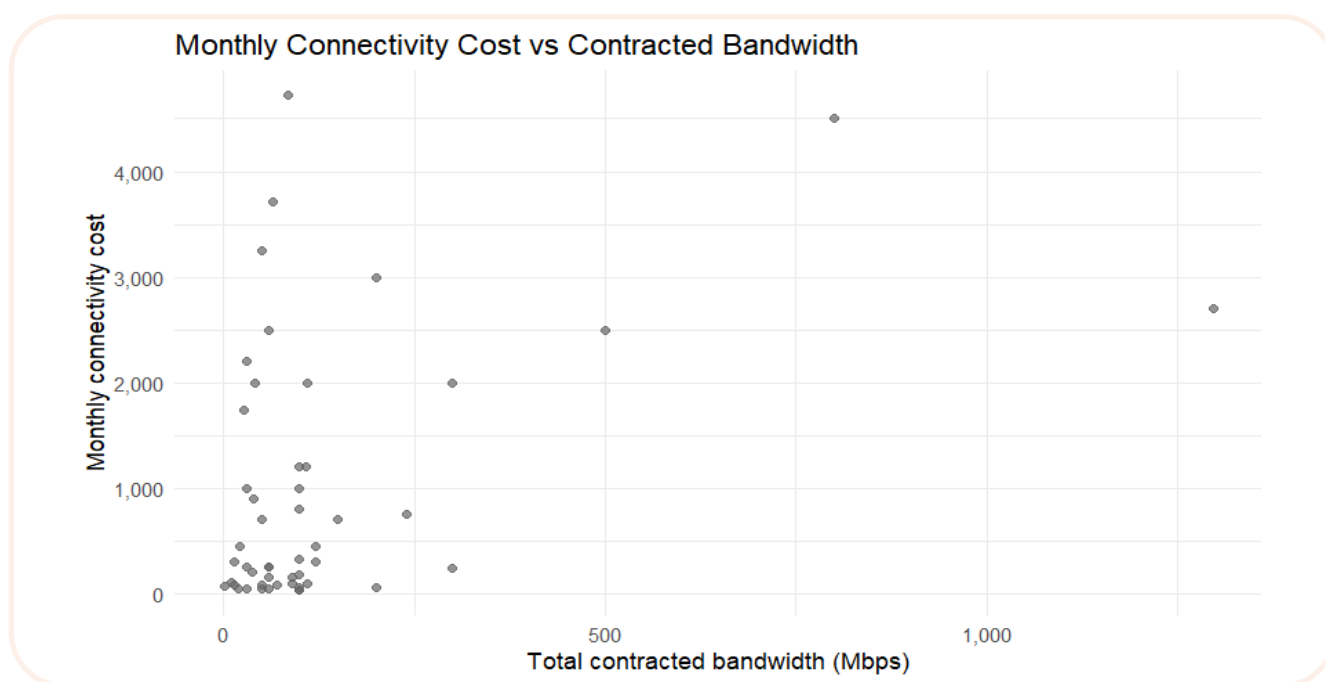


Figure 5: Monthly connectivity cost versus contracted bandwidth

The observed pattern reinforces the finding that affordability and efficiency, rather than basic access, are emerging constraints in the connectivity landscape, highlighting the potential value of pooled procurement and shared connectivity arrangements in reducing unit costs and improving value for money.

Campus network coverage (LAN and Wi-Fi)

Internal campus networking remains uneven and, in many cases, is limited in functionality. Just over half of institutions (54%) report having a local area network (LAN) covering the entire campus, suggesting that a significant proportion

of higher education institutions still lack wired networks that connect academic and administrative buildings. Among institutions with a LAN, coverage levels are generally high, with a median of 90% coverage across campus buildings (IQR

27.5%). This suggests a polarised pattern, with institutions tending to have either relatively comprehensive internal wiring or very limited deployment rather than an incremental rollout.

Table 8: Campus networking indicators.

Indicator	Summary
Institutions with campus-wide LAN	54%
LAN coverage across academic/admin buildings	90% (IQR 27.5%)
Institutions with campus-wide Wi-Fi	72%
Wi-Fi coverage across campus	4% (IQR 2%)

Although Wi-Fi availability appears to be more widespread, important constraints on access and use remain. Although 72% of institutions report having campus-wide Wi-Fi, this does not necessarily mean that students have open or universal connectivity. Discussions with institutional stakeholders suggest that Wi-Fi access is frequently limited to staff and administrative purposes, with little or no provision for students. In many institutions, internet access on campus is not freely available to students, and there are typically no institutional mechanisms through which students can purchase or subscribe to Wi-Fi services. Consequently, students often rely on their own mobile data to connect to the internet while on campus, even at institutions that formally report Wi-Fi availability.

The distinction between nominal availability and effective access is further reinforced by coverage depth. As Figure 6 shows, Wi-Fi coverage across campus spaces varies considerably. While some institutions report coverage of over 75% of campus areas, many fall within the 25–75% range, suggesting uneven deployment concentrated in offices, libraries, and administrative buildings rather than teaching and learning spaces. A small but significant proportion of institutions report coverage of less than 25% of campus areas.

Computing resources

Most institutions report having basic end-user computing infrastructure in place, particularly for students. **92% have dedicated student computer labs, with a median of two labs and 52 computers per institution.** This indicates a baseline level of shared access to computing resources, though the scale of provision varies according to institutional size.

Computing resources outside of student labs are comparatively limited. **The median number of computers in institutional libraries is one, whereas office and administrative environments report a median of 25 computers.** This suggests that access to dedicated computing equipment for staff, researchers or decentralised academic units may be limited.

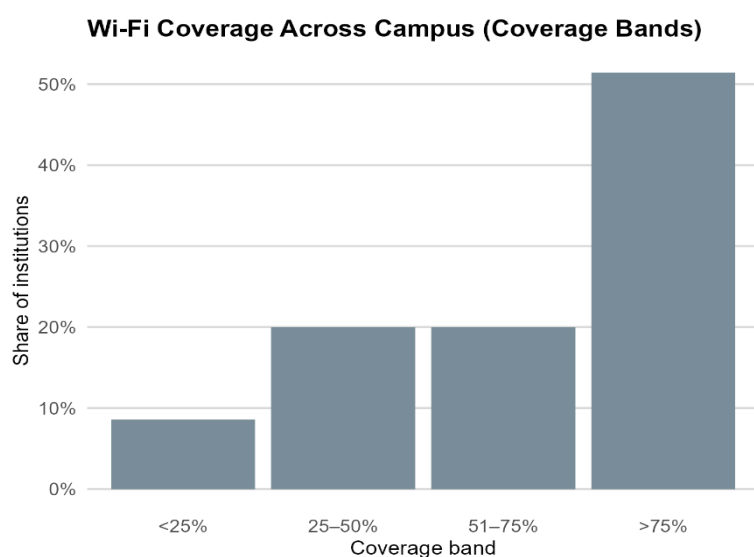


Figure 6: Wi-Fi coverage across campus

Table 9: Computing resources supporting learning and administration

Indicator	Summary	Comment
Institutions with dedicated student computer labs	92%	
Number of student computer labs (median)	2	
Total number of lab computers (median)	52.5	
Institutional computers in libraries (median)	1	
Institutional computers in offices/administration (median)	25.5	
Proportion of ICT equipment fully operational	>75%	

Institutions generally report that existing equipment is highly operational, with the most common response indicating that **more than 75% of ICT equipment is fully operational**. However, this indicator reflects self-reported functionality only and does not capture the age, performance or suitability of the equipment for more advanced digital applications.

Several institutions report very small numbers of non-lab computers, indicating uneven access for staff and non-teaching functions. The reporting of equipment condition is generally positive but lacks detail.

Power reliability

Power supply conditions appear to be relatively stable for ICT operations in most institutions, although resilience mechanisms vary. The most frequently reported occurrence of power interruptions affecting ICT services is “rarely”, which suggests that grid supply or primary power arrangements are generally adequate for day-to-day operations.

Table 10: Power and energy conditions affecting ICT operations

Indicator	Summary
Primary source of electricity for ICT infrastructure	Electricity grid
Frequency of power interruptions affecting ICT services	Rarely
Institutions with backup power for ICT systems	62%
Institutions using renewable or green energy for ICT	14%

However, only 62% of institutions report having backup power systems in place for ICT infrastructure. This implies that a significant minority remain vulnerable to service disruption during outages, even if such events are infrequent. Just 14% of institutions report using renewable or green energy sources for ICT, indicating that adoption of alternative energy remains limited.

The absence of backup power in a substantial proportion of institutions introduces uneven operational resilience, particularly for data systems and network equipment that require continuous uptime.

3.2.2 Readiness Indicators and Staging Logic

Readiness in ICT infrastructure and systems is assessed using a set of indicators that capture the presence of infrastructure, as well as the institutional capacity to operate, maintain and use it effectively. These indicators cover four interconnected components: internet connectivity, campus network infrastructure, computing resources and power reliability. Together, these components reflect the conditions under which digital systems can function consistently and at scale.

Connectivity indicators examine the following: whether institutions are connected to the internet; the technologies used; available and contracted bandwidth; service reliability; associated costs; and the use of monitoring tools to manage network performance. Campus networking indicators assess the existence and coverage of local area networks, backbone technologies, on-campus fibre deployment and wired and wireless coverage across academic and administrative buildings.

Computing resource indicators capture the availability and condition of institution-owned equipment, including computer laboratories, devices provided for teaching and learning, library services and administrative systems. They also consider whether devices meet the minimum requirements for current software and platforms, recognising the impact of outdated or non-operational equipment on digital adoption.

Power-related indicators evaluate the stability of the electricity supply for ICT operations. This includes assessing primary energy sources, the frequency of power interruptions, the availability of backup power solutions and the use of renewable or alternative energy sources, where applicable. Power reliability is considered a core element of infrastructure readiness rather than an external constraint.

The indicators within this domain are interpreted collectively in order to characterise institutional conditions in terms of a small number of readiness stages. These stages reflect the extent to which infrastructure is available, reliable, adequately resourced and integrated into institutional operations. Depending on the balance between connectivity, networking, equipment availability, and power resilience, institutions may occupy different readiness stages within this domain.

The staging logic is qualitative and comparative, informed by patterns across multiple indicators rather than mechanical scoring or weighted indices. This approach enables consistent interpretation across institutions while acknowledging variation in scale, context, and institutional priorities.

3.2.3 Distribution of Readiness Stages Across Institutions

Domain 1 readiness stages summarise the **scope and composition of foundational ICT infrastructure elements** across institutions, based on aggregated indicator scores. The staging reflects the **presence and robustness within institutions of core infrastructure components**, such as connectivity type, internal campus networks, shared computing resources, monitoring practices and power continuity, rather than the adequacy or performance of these components.

Distribution of readiness stages. Most institutions cluster in the middle of the distribution. 54% (27 institutions) are classified as “Developing”, which indicates that multiple foundational infrastructure components are present, but they are uneven in terms of their composition and institutional robustness. A further 40% (20 institutions) are classified as “Relative Strength”, reflecting a broader and more consistent infrastructure across the Domain 1 indicators. Only three institutions (6%) fall into the “Priority Area” category, indicating limited coverage of foundational infrastructure components relative to their peers.

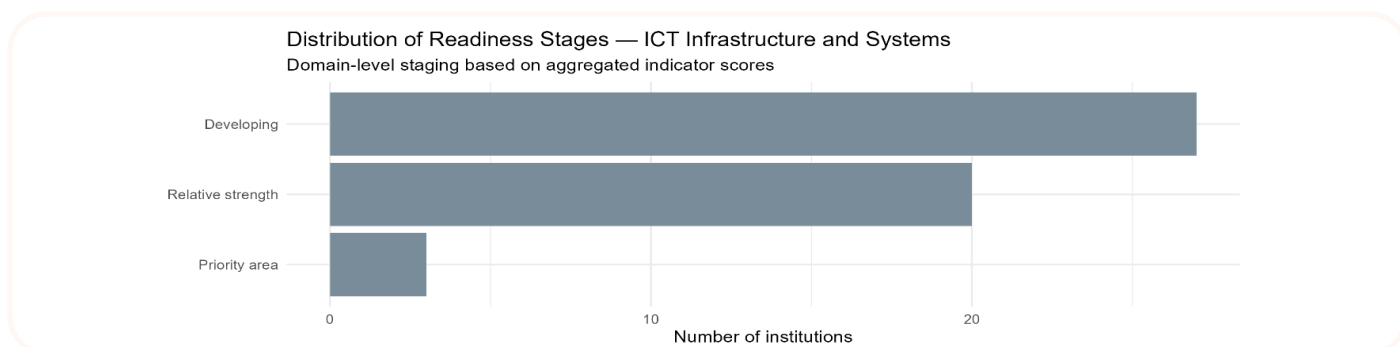


Figure 7: Distribution of readiness stages for ICT infrastructure and systems

Evidence coverage and staging confidence. Evidence coverage for Domain 1 is uniformly high. The median domain coverage is 1.0, with no institutions falling below full coverage and all reporting on the full set of six Domain 1 indicators. This suggests that the observed distribution reflects substantive variation in indicator scores rather than differences in response completeness or missing documentation.

Indicator breadth. All institutions report evidence for the full set of Domain 1 indicators, with a median of six indicators scored per institution (interquartile range (IQR) 0). Therefore, variation in staging arises from differences in indicator composition and scoring intensity rather than partial indicator coverage.

Interpreting Domain 1 stages.

- 01 Institutions classified as **"Relative Strength"** demonstrate a broader combination of institutional-grade infrastructure elements, such as structured internal networks, robust access technologies, shared computing resources and power continuity, across the Domain 1 indicators.
- 02 In contrast, **"Developing"** institutions typically report several foundational components, but with gaps in internal distribution, monitoring or resilience that limit their overall robustness.
- 03 Institutions flagged as a **"Priority area"** demonstrate limited coverage of these foundational components relative to the system as a whole.

It is important to note that these stages do not imply that institutions in the higher categories have adequate bandwidth relative to their size, reliable power or optimised internal coverage. These operational adequacy and performance considerations are addressed in the baseline analysis (Section 3.1.1).

Link to baseline conditions. The distribution observed here is consistent with baseline findings indicating near-universal basic connectivity, alongside substantial variation in internal networks, monitoring practices, power backup and effective capacity relative to user load. Therefore, Domain 1 staging highlights structural readiness differentials – the composition and institutionalisation of infrastructure – rather than service quality or performance outcomes.

System-level diagnostic implication. The Domain 1 results suggest that the primary infrastructure challenge facing Somali HEIs is no longer the absence of basic connectivity, but rather the uneven institutionalisation and resilience of infrastructure components. Strengthening internal distribution, monitoring and continuity mechanisms is likely to have a greater impact on system-wide readiness than expanding basic access alone.

3.2.4 Key Gaps and Internal Variations

The results for Domain 1 show that the main constraints are no longer the absence of basic connectivity, but rather the uneven institutionalisation of “institutional-grade” infrastructure elements, which determine whether digital services can be delivered reliably and on a large scale. The baseline conditions and readiness-stage distribution highlight three recurring gaps: performance visibility, internal distribution and resilience. There is also significant internal variation in effective capacity when institutional size is considered.

Monitoring and performance visibility remain limited. Although 100% of institutions report internet connectivity, only 28% report having internet monitoring mechanisms in place (see Table 4). This creates a consistent maturity gap across the system: institutions may have service access, but lack the operational tools and routines required to understand congestion and service quality, diagnose recurring problems, and hold providers accountable. This pattern helps to explain why a large proportion of institutions are categorised as “Developing” despite reporting connectivity and relatively low median downtime. Where monitoring is absent, reported reliability conditions are likely to be experienced unevenly by different users at different times, even if headline downtime figures appear modest.

The main source of institutional variation is internal network distribution. Internal campus networks are substantially less widespread than external connectivity. Only 54% of institutions report having a campus-wide LAN, even though LAN coverage is typically high among those that have one (median 90%, IQR 27.5%; see Table 8). This creates a polarised pattern whereby institutions either report near-complete wiring or very limited deployment. This implies that network-enabled services are concentrated in select buildings or administrative areas rather than being available across the entire institution. Wi-Fi is more widely reported (72%), but coverage depth varies (see Figure 6), with many institutions

operating in partial coverage bands. This uneven internal distribution is a key driver of the split between “Relative Strength” and “Developing” institutions in the staging results (Figure 7): the differentiator is not so much the existence of connectivity, but rather the extent to which it is distributed across teaching, learning and administrative spaces.

Effective Internet capacity is constrained when adjusted for institutional size. Bandwidth per user emerges as the most binding diagnostic constraint in the baseline analysis. The median institution reports a contracted bandwidth of 77.5 Mbps, but when this is divided by a median user base of 2,069, it equates to only 0.04 Mbps per user (Table 6). The distribution is highly skewed (**Error! Reference source not found.**), with most institutions clustered at very low per-user capacity levels, and only a small number of outliers reporting relatively high capacity. This implies that comparable headline bandwidth figures can correspond to very different user experiences depending on institutional size. It also clarifies why higher readiness-stage categories should not be interpreted as “adequate performance”: institutions may have well-developed infrastructure yet still face effective capacity constraints that limit the practical use of digital systems, particularly for concurrent access, media-rich content or online assessment.

Although computing resources are available, they are not evenly distributed beyond the labs. Most institutions report student labs (92%) and generally positive equipment functionality (with “fully operational” being the most common response, at over 75%; see Table 9). However, the median number of computers in libraries is just one, whereas administrative environments report a median of 25.5. This suggests that access is still primarily focused on labs, with limited distributed computing resources in learning commons, libraries or decentralised academic units. This variation is likely to be most significant for institutions where personal device ownership is low, or where digital workflows require broader access than is available during scheduled lab sessions.

Resilience measures are partial and uneven. Power interruptions affecting ICT services are most commonly reported as “rarely”, but only 62% of institutions report having backup power for ICT systems (Table 10). This means that a substantial minority remain exposed to service disruption during outages, even if such outages are infrequent, particularly for network equipment and institutional systems requiring continuous uptime. The limited use of renewable or green energy for ICT (14%) suggests that cost and operational continuity risks are primarily mitigated through conventional backup arrangements rather than alternative energy strategies.

The technology mix suggests differentiated reliability and scaling pathways. Fibre predominates (76%), but a significant proportion still report ADSL/DSL (28%) and microwave links (15%), with a small number relying on satellite-based services. This mix implies different risk profiles and scaling trajectories: institutions without fibre or redundancy options may be more exposed to variability in quality and downtime, which contributes to the outliers observed in reliability and capacity distributions.

Internal variations in Domain 1 readiness are less driven by whether institutions are connected, and more by how connectivity is managed, distributed and resilient, and whether bandwidth and device capacity remain usable at an institutional scale. These differences in readiness explain why institutions cluster in the “Developing” and “Relative Strength” categories despite exhibiting system-wide constraints in operational capacity and robustness.

3.2.5 Implications for Institutions

The findings from Domain 1 suggest that the main infrastructure challenge for most Somali HEIs is no longer access to basic connectivity, but rather the ability to operate infrastructure as a reliable, institution-wide service. Differences in monitoring, internal distribution, resilience, and effective capacity relative to institutional size determine the extent to which digital systems can be used consistently for teaching, learning, and

administration.

Limited performance visibility restricts operational control. With fewer than one-third of institutions reporting internet monitoring, it is likely that many are managing connectivity reactively rather than proactively. This restricts their capacity to diagnose service issues, manage congestion during peak periods or liaise with providers regarding performance, even when headline downtime appears modest.

Uneven internal networks result in uneven access. Partial LAN and Wi-Fi coverage means that, in principle, digital systems may be available but accessible only in selected buildings or labs. In such contexts, the adoption of institutional platforms tends to be fragmented, with digital services embedded in specific units rather than being used consistently across the institution.

Effective capacity, rather than headline bandwidth, is a limiting factor. The very low median bandwidth per user suggests that many institutions will struggle to support concurrent access to learning platforms, video-enabled teaching, and online assessments on a large scale. Larger institutions with similar contracted bandwidths face tighter constraints on a per-user basis than their smaller peers, which highlights the importance of capacity adjusted for scale in institutional planning.

Access to computing remains concentrated. Although student labs are common, the limited availability of institutional devices in libraries and decentralised spaces implies a continued reliance on scheduled lab use and personal devices, which can restrict inclusive access to digital services.

Resilience gaps affect service continuity. The absence of backup power in many institutions increases their vulnerability to disruptions affecting networks and systems, even if power interruptions are infrequent.

Domain 1 results suggest that institutional digital readiness is more dependent on the management, distribution and safeguarding of existing infrastructure

thanonacquiringadditionalinfrastructure. Those classified as “Relative Strength” are better placed to provide stable, institution-wide digital services, whereas “Developing” institutions face operational constraints that restrict the reliability and scope of digital systems, despite having many foundational components in place.

3.3 Human Resources and Institutional Capacity

This domain examines the human and organisational capacity required to plan, operate and maintain institutional ICT infrastructure and digital systems. The focus is on the structure of ICT functions, staffing levels and role coverage, technical qualifications, operational practices and institutional arrangements that support effective ICT service delivery.

The assessment considers whether institutions have formally established ICT units, and where these units sit within institutional governance structures. Staffing profiles across key technical and managerial roles are examined, including systems administration, network engineering, technical support and ICT leadership, to evaluate the adequacy and balance of internal capacity.

Indicators also address the qualifications and skills of ICT staff, including the prevalence of formal ICT training and professional certifications, as well as access to ongoing professional development. The assessment considers whether institutions allocate resources for ICT staff training and whether there are mechanisms in place to support upskilling in response to evolving technologies and systems.

Operational capacity is evaluated based on institutional practices for ICT support and maintenance. This includes the use of service management tools, procedures for handling user support requests, the implementation of preventive maintenance routines and written standard operating procedures for managing ICT systems. The domain also examines the extent to which institutions rely on third-party providers for ICT services, as well as the types of functions that are outsourced.

Finally, the domain considers issues of staff turnover, recruitment, and retention. Indicators capture vacancy levels, recruitment constraints and strategies for retaining qualified ICT personnel. It recognises that sustained institutional capacity depends on more than just staffing levels, but also on continuity, incentives and career development opportunities.

3.3.1 Baseline Conditions Across Somali HEIs

The majority of surveyed institutions report having a formally established ICT unit, indicating that ICT functions are recognised within institutional structures rather than being handled on an ad hoc basis. However, the positioning of the ICT function within senior management varies. In many cases, ICT reports to administrative or finance leadership rather than to the institution’s chief executive, which affects how ICT priorities are set and resourced.

Table 11: ICT organisational structures and reporting lines

Indicator	Summary
Institutions with a formally established ICT unit	84%
Primary reporting line of the ICT function	Deputy Vice-Chancellor (Administration/ Finance)

The presence of an ICT unit does not uniformly translate into staffing depth. **Institutions report having a median of one small ICT team**, with staffing levels varying widely once institutional size and complexity are taken into account. While most institutions report having at least one ICT technician, fewer report the presence of specialised roles such as systems administrators, network engineers or ICT managers. This suggests that ICT functions in many institutions are concentrated in generalist roles with limited differentiation of roles.

Table 12: ICT staffing presence and role composition

Indicator	Summary
Total ICT staff per institution	7 (IQR 5.5)
Institutions with at least one ICT technician	100%
Institutions with at least one systems administrator	93%
Institutions with at least one network engineer	95%
Institutions with at least one ICT manager or director	88%

Technical staffing profiles indicate that routine support and basic system maintenance are more commonly covered than higher-level functions such as network design, systems architecture or strategic ICT management. The presence of a designated ICT manager or director is not universal, which points to potential gaps in leadership capacity within ICT units, particularly as digital systems expand in scope and importance.

Operational support practices further illustrate the maturity of ICT organisations within institutions. Just over half of institutions report using at least one formal ICT support system, such as a helpdesk, monitoring tool or asset management system. Where such systems exist, they are often used only partially rather than comprehensively.

Table 13: ICT operational support practices

Indicator	Summary
Institutions using formal ICT support systems	66%
Primary method for handling ICT support requests	Informal (email or phone)
Institutions implementing preventive maintenance routines	50%
Institutions with written ICT SOPs	48%
Institutions outsourcing any ICT functions	50%

When it comes to handling user support requests, informal mechanisms

such as direct emails or phone calls remain commonplace. Furthermore, a significant proportion of institutions report having no structured process whatsoever. Some institutions report preventive maintenance practices, but these are not yet standardised across the system. Similarly, written standard operating procedures (SOPs) for ICT are not widespread, which limits institutional continuity and knowledge transfer, particularly in contexts of staff turnover.

A subset of institutions report outsourcing ICT functions, typically for specialised services or infrastructure management. While this suggests a degree of pragmatic adaptation to internal capacity constraints, it also introduces dependencies that require oversight and coordination capacity within the institution itself.

Overall, the baseline evidence suggests that ICT is institutionally recognised, but unevenly embedded. Although formal structures exist in many institutions, staffing depth, role specialisation and operational systems often fail to keep pace with the growing demands placed on ICT units. This suggests that organisational and human resource constraints, rather than the absence of ICT units per se, are a key limiting factor in institutional digital readiness.

3.3.2 Readiness Indicators and Staging Logic

Readiness in terms of human resources and institutional capacity is assessed using indicators that capture the organisation, adequacy and sustainability of ICT staffing and support functions. These indicators address four interrelated dimensions: the institutional structure of the ICT function; staffing levels and role coverage; staff qualifications and professional development; and operational practices for ICT service delivery.

Those related to institutional structure assess whether ICT functions are formally established, the reporting line of the ICT unit and whether there are defined leadership roles responsible for ICT strategy and operations. These indicators reflect the extent to which ICT is recognised as a core institutional function with clear accountability.

Staffing and role coverage indicators examine the number and distribution of ICT personnel across technical, administrative and managerial roles. Attention is given to the presence of key competencies such as systems administration, network management, user support and ICT leadership, as well as the extent to which unfilled positions may constrain operations.

Qualifications and skills indicators capture the proportion of ICT staff with formal ICT training, professional certifications and access to ongoing training and professional development. The assessment also considers whether institutions allocate dedicated resources for ICT staff development, recognising the importance of continuous skill development in sustaining digital systems.

Operational practice indicators evaluate the delivery and maintenance of ICT services. These include the use of service management systems, procedures for handling user support requests, the implementation of preventive maintenance routines and the availability of written standard operating procedures. The extent and nature of the outsourcing of ICT functions are also considered as part of the overall capacity profile.

The indicators within this domain are interpreted collectively in order to characterise institutional conditions along a small number of readiness stages. These stages reflect the extent to which ICT functions are formally organised, adequately staffed, professionally supported and embedded in institutional processes. Depending on the balance between staffing adequacy, skills depth, operational practices, and staff retention, institutions may occupy different readiness stages within this domain.

The staging logic is qualitative and comparative, informed by patterns across multiple indicators rather than mechanical scoring. This approach facilitates a consistent interpretation of institutions while acknowledging contextual constraints and variations in scale and resources.

3.3.3 Distribution of Readiness Stages Across Institutions

Domain 2 readiness stages summarise the **institutionalisation of ICT human resources and organisational structures**. This includes the presence of formal ICT units, staffing roles, operational support practices and basic organisational processes for ICT service delivery. The staging reflects structural capacity and organisational embedding rather than the depth of staff skills or the effectiveness of services.

Distribution of readiness stages. The majority of institutions are classified as having relative strength in this domain. 76% (38 institutions) fall into this category, indicating that core organisational elements, such as an identifiable ICT function, designated staff roles and basic operational practices, are present in most institutions. A further 8% (4 institutions) are classified as “Developing”, reflecting partial or uneven organisational arrangements. 16% (8 institutions) are flagged as a Priority area, signalling limited formalisation of ICT roles or organisational support structures relative to peers.

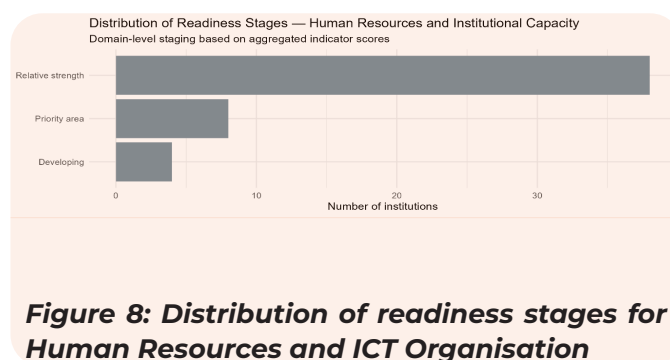


Figure 8: Distribution of readiness stages for Human Resources and ICT Organisation

Evidence coverage and staging confidence. Evidence coverage for Domain 2 is high but not uniform. The median domain coverage is 1.0, with an interquartile range of 0.25 and a minimum observed coverage of 0.5. This indicates that, although most institutions provided evidence across all Domain 2 indicators, some reported on only part of the indicator set. The resulting distribution therefore reflects variation in organisational capacity, as well as the uneven documentation or visibility of certain human resource and operational practices.

Indicator breadth. Domain 2 comprises four indicators. Institutions report a median of four indicators (IQR 1) scored, with a minimum of two scored among some institutions. This suggests that differences in readiness stages are primarily driven by the completeness and formalisation of organisational arrangements rather than by the complete absence of ICT staff.

Interpreting Domain 2 stages:

- 01 Institutions classified as **“Relative Strength”** typically report the existence of a formal ICT unit or function, identifiable ICT staffing roles and basic operational support practices, such as maintenance routines or defined request-handling mechanisms.
- 02 **Developing** institutions often demonstrate partial organisational capacity, for example, having ICT staff without clear managerial roles or relying on informal support practices.
- 03 Institutions flagged as a **Priority area** demonstrate limited formalisation of ICT human resources, including gaps in dedicated staffing, documented procedures and structured operational support.

As with other domains, these stages should not be interpreted as a measure of staff sufficiency, skill depth, or service quality. The assessment does not evaluate whether staffing levels are adequate relative to institutional size, nor does it assess advanced competencies or professional development outcomes.

Link to baseline conditions. Domain 2 distribution aligns with baseline findings showing a widespread presence of ICT staff and organisational units alongside variability in formalisation, documentation and operational practices. High classification rates in this domain reflect the existence of organisational structures, even where those structures operate with limited resources or strategic authority.

System-level diagnostic implications. The results suggest that basic organisational capacity for ICT is largely in place across Somali HEIs, but that the depth and

consistency of these arrangements varies. Therefore, the main constraint is not the absence of ICT personnel per se, but rather the uneven formalisation and institutional embedding of ICT roles and operational practices. This may limit the ability to scale up and be resilient as digital demands increase.

3.3.4 Key Gaps and Internal Variations

The results of Domain 2 suggest that the majority of Somali HEIs have moved beyond fully ad hoc ICT arrangements. 84% of HEIs reported having a formally established ICT unit (Table 11), and relatively high rates of role coverage were reported across technician, systems administration, and network engineering functions (Table 12). However, the baseline findings and the distribution of readiness stages suggest that constraints mainly lie in organisational embedding, operational maturity and inconsistent documentation of human resource and service management practices rather than in the mere existence of ICT staff or units.

The strategic positioning and authority of the ICT function varies. The most common reporting line for ICT is the Deputy Vice-Chancellor (Administration/ Finance) rather than the institution’s chief executive (see Table 11). This suggests that ICT is often primarily positioned as an administrative support function rather than as a cross-cutting institutional capability. In practice, this can influence prioritisation, budget negotiation and the extent to which ICT is integrated into broader institutional decision-making processes. Therefore, the high proportion of institutions classified as “Relative Strength” reflects structural presence rather than strategic authority or leadership influence of ICT units.

Although role presence appears strong, depth and differentiation remain uncertain. Institutions report a median of seven ICT staff (interquartile range (IQR) 5.5), and large majorities report having at least one systems administrator (93%), network engineer (95%), and ICT manager/director (88%) (see Table 12). While these figures suggest a broad presence of roles, they may mask variations in whether

these roles are full-time, whether individuals cover multiple functions and whether specialised competencies are consistently available. The baseline narratives suggest that many ICT functions are concentrated within generalist roles, which can restrict higher-level functions such as systems architecture, network planning, cybersecurity oversight and the lifecycle management of institutional platforms. This likely contributes to the presence of “Developing” and “Priority Area” institutions, despite the generally positive signals regarding role coverage.

Operational service management practices are inconsistent and often informal. Although 66% of institutions report using at least one formal ICT support system, the most common approach to handling ICT support requests remains informal (email or phone), and a significant proportion report having no structured process (see Table 13). Only 50% of institutions report performing preventive maintenance, and only 48% have written SOPs (Table 13). This indicates a gap in maturity between having ICT personnel and operating ICT services through standardised, auditable routines. The uneven adoption of service management practices is a key internal differentiator: institutions with similar staffing profiles may differ substantially in terms of service reliability and institutional continuity, depending on whether or not procedures and support systems are institutionalised.

Although outsourcing reflects adaptive capacity, it introduces coordination requirements. Around half of institutions (50%; Table 13) report outsourcing some ICT functions. While this can alleviate internal capacity constraints, particularly with regard to specialised infrastructure or systems support, it also creates dependencies that necessitate internal oversight, such as vendor management, service-level monitoring, and integration with institutional workflows. Where monitoring tools and standard operating procedures (SOPs) are limited, outsourcing can increase operational risk rather than reduce it. This reinforces the importance of internal organisational maturity, even where services are externally supported.

Evidence coverage and visibility gaps

affect the interpretation of “Relative Strength”. Domain 2 has high but uneven evidence coverage (median coverage 1.0; minimum 0.5), indicating that some institutions did not report on all indicators. This suggests that some of the variation in staging reflects limited documentation or visibility of practices such as SOPs, preventive maintenance routines or support systems rather than a clear absence of them. It also implies that the large proportion of institutions classified as “Relative Strength” indicates the presence of basic organisational elements rather than consistent operational maturity across institutions.

Internal variation in Domain 2 readiness is driven by differences in how ICT functions are embedded and operated, such as reporting lines and authority, the extent of role differentiation, and whether ICT service delivery is supported by formal processes and documentation. These gaps help to explain why the distribution shows high “Relative Strength” alongside a significant “Priority Area” group, and why organisational capacity is best understood as being present, but inconsistent and uneven in maturity.

3.3.5 Implications for Institutions

The findings of Domain 2 imply that, while most Somali HEIs have an identifiable ICT function and basic staffing roles in place, institutional readiness increasingly depends on how ICT is positioned, managed and sustained as a service-delivery capability. The high proportion of institutions classified as “Relative Strength” reflects a structural presence and basic organisational embedding rather than an assured adequacy of staffing levels, skill depth, or service quality.

Variation in ICT reporting lines suggests different levels of strategic influence. As the ICT function most commonly reports through administrative or finance leadership, ICT may be treated primarily as a support function rather than a cross-cutting institutional capability. This can affect prioritisation, decision-making speed and the ability of ICT units to coordinate academic and administrative functions as digital systems expand.

Staffing profiles suggest functional coverage, but also potential reliance on generalists. While most institutions report the presence of key roles, typical ICT team sizes and likely responsibilities overlap, meaning continuity and specialisation may be fragile, particularly for higher-level functions such as systems architecture, network planning, security oversight and platform lifecycle management. Consequently, institutions may experience constraints in sustaining and scaling institutional platforms rather than in day-to-day troubleshooting.

Operational maturity is a critical differentiator. Continued reliance on informal support channels, partial use of service management systems and limited preventive maintenance routines and written SOPs suggest institutions may experience avoidable service interruptions, inconsistent user support and weak institutional memory during staff turnover. Even where ICT units exist, a lack of documented processes reduces resilience and makes ICT performance more dependent on individual staff members.

While outsourcing can reduce the immediate workload, it increases coordination demands. Institutions that outsource ICT functions require internal capacity for oversight, vendor management, and integration with institutional workflows. Where monitoring tools and SOPs are limited, outsourced services may create dependencies that are challenging to manage, thereby affecting service continuity and accountability.

Domain 2 results suggest that institutions would benefit most from clear authority, defined roles, and standardised operational practices within ICT functions. For many institutions, the limiting factor is not so much the existence of ICT staff as the consistency, documentation and institutional embedding of ICT service delivery as digital demands grow.

3.4 ICT Governance, Policy and Strategic Planning

This domain evaluates the institutional frameworks that direct the decision-making, planning and oversight processes of ICT within higher education institutions. The focus is on whether ICT is managed as a strategic institutional function, supported by formal strategies, policies and governance mechanisms.

The assessment looks at whether institutional ICT strategies or master plans exist, have been approved, and are up to date, and how aligned they are with overall institutional strategic plans. Indicators capture whether strategies are supported by defined implementation roadmaps, timelines and mechanisms for tracking progress against planned initiatives. These elements provide insight into the extent to which ICT planning is structured, forward-looking and actionable.

The presence and scope of key ICT-related policies are used to assess institutional policy frameworks, including those covering acceptable use, cybersecurity, data protection, procurement, asset management, service management, and backup and disaster recovery. The frequency with which policies are reviewed and updated is also considered, reflecting the institution's capacity to adapt its governance arrangements as digital systems evolve.

Governance mechanisms are examined through the existence and functioning of ICT steering committees or equivalent bodies. The indicators address committee composition, leadership, meeting frequency, and decision-making authority over ICT policies and budgets. These factors indicate the degree to which senior management is engaged with and accountable for ICT oversight.

The domain also considers whether institutions integrate national or regional digital education priorities into their ICT plans, and whether there are mechanisms in place to monitor ICT performance and service delivery. The use of user satisfaction surveys and internal or external ICT reviews is also assessed as evidence of institutional learning and continuous improvement.

3.4.1 Baseline Conditions Across Somali HEIs

The ICT governance and planning arrangements reported by Somali HEIs show a clear split between (i) those that have formal strategies and policy instruments, and (ii) those where governance and documentation are partial or not readily verifiable. 60% of institutions report having an official ICT strategy or master plan. Where strategies exist, they are usually formalised: 90% have been formally approved, and 83% have an implementation roadmap. In contrast, however, only 29% of institutions report having an ICT steering committee or an equivalent body, which suggests that standing oversight mechanisms are less common than strategy documents.

Table 14: ICT strategy and planning indicators

Indicator	Summary
Institutions with an official ICT strategy or master plan	60%
ICT strategies that are formally approved	90%
Perceived alignment between ICT strategy and institutional strategy	Very aligned
Institutions with a defined ICT implementation roadmap	83%

ICT strategy and planning

A majority of institutions report a formal ICT strategy or master plan (60%). Among institutions with a strategy, formal approval is high (90%), suggesting that ICT strategies are often recognised as official institutional instruments when developed. The perceived alignment between ICT strategy and institutional strategy is commonly reported as “very aligned” (modal response), implying that institutions generally view ICT plans as supporting core institutional goals rather than as technical plans in their own right. Most institutions with a strategy also report having a defined implementation roadmap (83%), indicating that planning often extends beyond a high-level vision to include specific activities.

These patterns suggest comparatively strong “front-end” planning among

institutions with strategies. The remaining institutions – those without an ICT strategy – represent a substantial segment of the system where ICT development is likely to be guided more by immediate operational needs and procurement cycles than by structured transformation planning.

ICT policy framework

Formal ICT-related policies are widely reported. 82% of institutions report having at least one such policy. However, this metric includes cases where a policy is reported to exist, yet it is neither documented nor readily shared. This suggests that “policy presence” should be viewed as an indication of intent or awareness, rather than as verifiable documentation.

Institutions report a **median of six ICT policy areas covered** out of twelve possible areas (IQR 7). The wide IQR suggests substantial variation in policy breadth with some institutions reporting extensive policy coverage, while others cover only a few areas.

Table 15: ICT policy framework (policy presence and breadth)

Indicator	Summary
Institutions with at least one formal ICT-related policy	82%
Number of ICT policy areas covered per institution	6 (IQR 7)

This distribution indicates the uneven institutionalisation of ICT rules and controls. Where coverage is limited or documentation is lacking, institutions may struggle to maintain consistent practices across procurement, user access, service management and risk controls.

The existence of a policy does not confirm its quality, currency, communication, enforcement or integration into operational workflows. In this baseline section, policy indicators are treated as signals of documentation and visibility rather than as signals of audited compliance.

Policy coverage by policy type

Coverage differs significantly across specific policy areas. Several foundational policy types are reported by at least half of institutions, including Data Protection/Privacy (62%), Policy for Staff and Student Email Accounts (60%), and Acceptable Use Policy (58%). Operational policies, such as ICT asset management (56%) and backup/

disaster recovery (50%), are also reported by approximately half of institutions. In contrast, policies governing device usage and digital pedagogy are less commonly reported, including BYOD/mobile device policies (32%) and open educational resources (OER)/digital content policies (32%).

Table 16: ICT policy coverage by policy type

Indicator	Proportion
Acceptable Use Policy (AUP) for ICT	58%
Cybersecurity or Information Security Policy	40%
Data Protection or Privacy Policy	62%
Procurement Policy for ICT	46%
Bring Your Own Device (BYOD) or Mobile Device Policy	32%
Open Educational Resources or Digital Content Policy	32%
Social Media Use in Teaching and Learning	50%
Policy for Staff and Student Email Accounts	60%
ICT Asset Management Policy	56%
ICT Helpdesk/Service Management Policy	42%
ICT Risk Management Policy or Framework	40%
Backup and Disaster Recovery Policy	50%

The profile suggests that institutions more frequently formalise policies tied to basic service provision and user controls, while fewer report coverage in areas requiring stronger coordination across academic, administrative and security functions (e.g. BYOD governance, content/OER policy frameworks and formal ICT risk management).

As the survey records the existence of policies at institutional level (including

cases where policies are not documented or shared), reported coverage should not be taken as confirmation that policies are consistently implemented across faculties and campuses. This limitation is reinforced by the limited prevalence of ICT performance monitoring and audit practices reported elsewhere in this section. Follow-up validation is needed in later stages to distinguish documentation from operationalisation.

ICT governance structures and monitoring mechanisms

Few institutions report having formal governance bodies. **Only 30%** report an ICT steering committee or equivalent body. Where such committees exist, the Vice-Chancellor/President/Rector/Principal is most commonly reported as the chair, indicating that, when constituted, governance is often anchored at the top executive level.

Among institutions with a committee, **80% report that the committee has decision-making authority over ICT budgets or policies.** This suggests that, when present, committees are often empowered rather than purely advisory. **Table 17: ICT governance structures and decision authority**

Indicator	Summary
Institutions with an ICT steering committee or equivalent body	30%
Chairing authority of the ICT governance committee	Vice-Chancellor/ President/ Rector/ Principal
Committees with decision-making authority over ICT budgets or policies	80%

The contrast between the relatively common reporting of strategy and policy and the limited prevalence of steering committees suggests that ICT oversight in many institutions may occur

through informal executive channels, administrative management structures or ad hoc committees, rather than standing governance arrangements or systematic performance monitoring mechanisms. This can limit continuity of oversight, reduce predictability in prioritisation and investment decisions, and weaken feedback loops between implementation experience and strategic revision.

The effectiveness of governance depends as much on composition as existence. Committee structures that include finance/procurement, academic leadership, quality assurance (QA), student administration and ICT security functions are more likely to reflect institution-wide priorities and risks than committees dominated by ICT unit staff alone.

Signals from monitoring, review and organisational learning

Evidence on monitoring and review mechanisms indicates uneven institutional learning capacity. **Only 38% of institutions report having mechanisms in place to monitor ICT performance and service delivery.** This indicates that routine visibility into system performance is absent in most institutions.

User feedback mechanisms are more common, but inconsistent. **Half of institutions report having conducted user satisfaction surveys within the past three years.** This suggests that, while some institutions have systematic feedback from students and staff, this is not yet embedded as a standard management practice across the system.

Table 18: Monitoring, feedback and review mechanisms

Indicator	Yes (%)	No (%)	Don't know (%)
Institutions with mechanisms to monitor ICT performance and service delivery	38%	60%	2%
Institutions that conducted user satisfaction surveys in the past 3 years	50%	44%	6%
Institutions that conducted internal or external ICT audits/reviews in the past 3 years	28%	72%	0%

Formal review and assurance processes are the least prevalent. Only 28% of institutions report having conducted internal or external ICT audits or reviews

in the past three years. The absence of recent audits in most institutions limits the availability of independent assessments of ICT risks, controls and performance.

3.4.2 Readiness Indicators and Staging Logic

Readiness in ICT governance, policy and strategic planning is assessed using indicators that measure the formality, coherence and effectiveness of institutional decision-making and oversight arrangements. These indicators are organised around four interrelated dimensions: strategic planning; policy frameworks; governance structures; and monitoring and review practices.

Strategic planning indicators assess whether institutions have formally approved ICT strategies or master plans, how recently these documents were approved, how aligned they are with institutional strategic plans, and whether implementation roadmaps with defined timelines exist. The extent to which planned ICT initiatives have been implemented provides additional insight into the transition from planning to execution.

Policy framework indicators examine the presence and scope of key ICT-related policies, including those governing acceptable use, cybersecurity, data protection, procurement, asset management, service management and business continuity. Attention is also given to how frequently policies are reviewed and updated, reflecting the institution's ability to maintain relevant and enforceable governance instruments.

Governance structure indicators focus on the existence and functioning of ICT steering committees or equivalent bodies. These indicators assess committee composition, leadership, meeting frequency, and decision-making authority over ICT policies and budgets. Together, these indicators reflect the extent of senior management engagement and institutional accountability for ICT governance.

Monitoring and review indicators capture whether institutions track ICT performance and service delivery, conduct user satisfaction surveys, or undertake internal or external ICT reviews or audits. These practices are considered signals of institutional learning and continuous improvement, rather than compliance

requirements.

The indicators within this domain are interpreted collectively in order to characterise institutional conditions in terms of a small number of readiness stages. These stages reflect the degree to which ICT governance and planning are formalised and integrated into institutional management, as well as being supported by active oversight and review mechanisms. Depending on the maturity and coherence of their strategic, policy, and governance arrangements, institutions may occupy different readiness stages.

The staging logic is qualitative and comparative, informed by patterns across multiple indicators rather than mechanical scoring. This approach facilitates a consistent interpretation of institutions while accommodating differences in size, governance structures and resource constraints.

3.4.3 Distribution of Readiness Stages Across Institutions

Domain 3 readiness stages summarise the institutionalisation of ICT governance, policy frameworks and strategic planning arrangements. This includes the existence of formal ICT strategies and the breadth of policies across core governance areas. It also includes governance bodies and monitoring or review mechanisms. The staging reflects the maturity of governance structures and documentation, rather than the effectiveness or enforcement of policies.

Distribution of readiness stages. The distribution for Domain 3 is skewed towards the lower and middle stages, highlighting governance as a persistent, systemic constraint. 40% of institutions (20) are classified as “Developing”, indicating the presence of partial governance arrangements that are incomplete or uneven. A further 34% (17 institutions) are classified as a Priority area, reflecting the limited formalisation of ICT governance and policy frameworks compared to those of their peers. Only 26% (13 institutions) are classified as “Relative Strength”, demonstrating comparatively more comprehensive governance structures across the Domain 3 indicators.

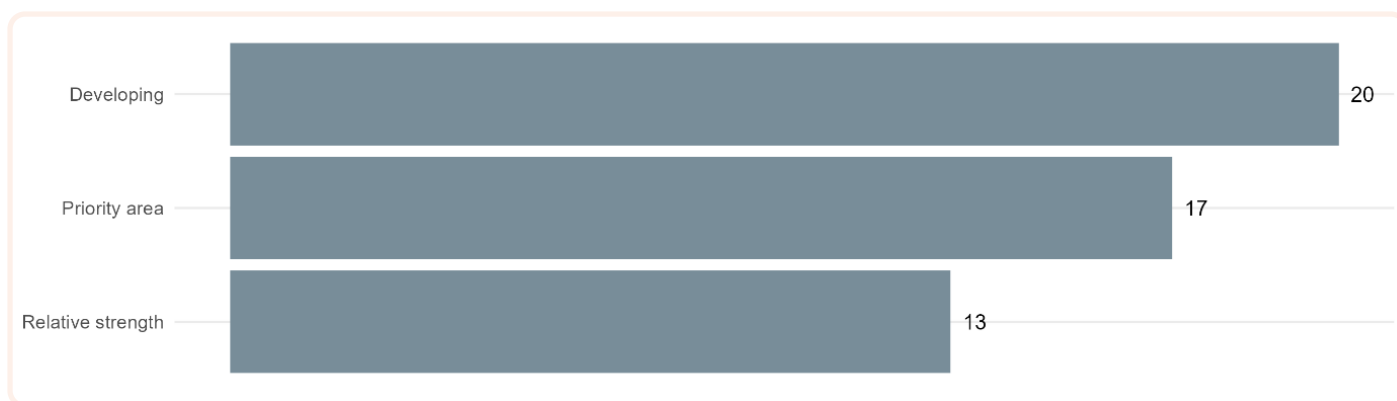


Figure 9: Distribution of readiness stages for ICT governance, policy and strategic planning

Evidence coverage and staging confidence. Evidence coverage for Domain 3 is high overall, with a median domain coverage of 1.0 indicating that most institutions provided information across the full set of indicators. However, the IQR of coverage (0.25) and the minimum observed coverage (0.75) suggest that the documentation and visibility of governance artefacts remain uneven. The observed staging therefore reflects genuine variation in governance maturity, as well as differences in the formal documentation of governance practices.

Indicator breadth. Domain 3 comprises four indicators, with institutions reporting a median of four scored indicators (IQR 1). A small number of institutions report evidence for only three indicators. Therefore, variation in readiness stages is primarily driven by differences in policy breadth, governance formalisation and strategic alignment rather than by a complete absence of governance activity.

Interpreting Domain 3 stages:

- 01** Institutions classified as “**Relative Strength**” typically demonstrate a combination of formal ICT strategies, broader coverage of institution-wide ICT policies, and identifiable governance or oversight mechanisms. These institutions tend to exhibit more complete governance frameworks, even where implementation capacity may be limited.
- 02** In contrast, **Developing** institutions often report the existence of some governance components, such as an ICT strategy or isolated policies,

but lack comprehensive policy coverage or consistent governance structures.

- 03** Institutions flagged as a **Priority area** generally demonstrate limited policy breadth, weak or absent governance arrangements, and a reliance on informal planning processes.

As in other areas of this assessment, Domain 3 stages do not imply the effective enforcement, resourcing or operational impact of governance instruments. The assessment captures the existence and coverage of instruments, not their implementation quality or outcomes.

Link to baseline conditions. The Domain 3 distribution closely aligns with the baseline findings, which show a relatively widespread reporting of ICT strategies, in contrast to the more limited and uneven policy frameworks, governance bodies and monitoring practices. The concentration of institutions in the “Developing” and “Priority” area categories reflects the fact that strategic intent often precedes the comprehensive institutionalisation of governance, particularly in settings where resources are limited.

System-level diagnostic implications. At a system level, the results suggest that ICT governance continues to hinder digital transformation across Somali HEIs. While a minority of institutions demonstrate relatively mature governance frameworks, most lack the policy breadth and formal oversight mechanisms required to guide ICT investments coherently and sustainably. Unless addressed, weaknesses in governance are likely to limit the returns from infrastructure,

systems, and emerging technology investments.

3.4.4 Key Gaps and Internal Variations

The results for Domain 3 point to a governance maturity gap, characterised by stronger “front-end” documentation (strategies and selected policies) in some institutions, but weak or inconsistent institutional mechanisms for oversight, implementation discipline and organisational learning. The readiness-stage distribution, in which 40% of institutions are classified as “Developing” and 34% as a priority area, reflects the uneven institutionalisation of governance instruments and the limited prevalence of standing accountability structures.

The uneven presence of strategies creates a split between planned and reactive ICT development. 60% of institutions report having an ICT strategy or master plan. Among these, formal approval (90%) and the presence of an implementation roadmap (83%) are common (see Table 14). This suggests that, where they exist, strategies are often treated as official instruments. However, the remaining 40% represent a substantial segment of the system in which ICT decision-making is likely to be shaped more by immediate operational needs and procurement cycles than by structured transformation planning. This split directly contributes to the observed clustering in the lower and middle readiness stages.

Policy breadth varies widely, and documentation is not consistently verifiable. While 82% report at least one ICT-related policy, the median institution covers only six out of twelve policy areas, with a wide interquartile range (IQR) of seven (Table 15). This indicates significant internal variation in policy coverage: some institutions report extensive frameworks, while others report only a small number of policies. Additionally, the baseline notes that policy “existence” sometimes encompasses cases where policies are undocumented or unshared, meaning the indicator is best interpreted as visibility and intent rather than verified institutional control. This uneven documentation and visibility likely contributes to the priority area classification for institutions whose

governance is present in practice.

Policy coverage is concentrated in basic user controls and service administration, with gaps in areas requiring cross-functional coordination. Around half or more of institutions report several foundational policies, including Acceptable Use Policies (AUPs) (58%), data protection/privacy policies (62%), email account policies (60%), asset management policies (56%), backup/disaster recovery policies (50%), and social media use policies (50%) (Table 16). By contrast, fewer institutions report cybersecurity/information security policies (40%), ICT risk management frameworks (40%), BYOD policies (32%) and OER/digital content policies (32%). This suggests that institutions more frequently formalise rules tied to immediate service operations and user access, while fewer formalise policies that depend on coordinated governance across academic leadership, procurement/finance, security oversight, and digital pedagogy.

Standing governance bodies are uncommon, which weakens continuity and accountability. Only 30% of institutions report having an ICT steering committee or equivalent body (Table 17). This represents a significant structural discrepancy given the prevalence of strategy documents and individual policies. Where committees exist, they are typically chaired at the highest executive level and most have decision-making authority over budgets or policies (80% of committees), indicating that, when constituted, formal governance bodies are often empowered rather than merely symbolic. Therefore, the internal variation lies not only in the presence of committees, but also in the fact that institutions without such bodies may rely on informal executive channels or ad hoc structures. This limits continuity of oversight and institutional memory over time.

Constraints on organisational learning remain due to limited monitoring, feedback and independent review mechanisms. Only 38% of institutions report having mechanisms in place to monitor ICT performance and service delivery, and just 28% report having conducted internal or external ICT audits

or reviews in the past three years (see Table 18). While 50% of institutions report conducting user satisfaction surveys, indicating that some have begun to institutionalise feedback, this is not yet consistent across the system. This pattern highlights a significant maturity gap: while governance artefacts may exist, routine feedback loops and independent assurance mechanisms are not widespread. Without such mechanisms, institutions have limited capacity to learn systematically from implementation experience, update strategies and policies, or identify control weaknesses before incidents occur.

Evidence visibility remains a significant source of variation. Domain 3 has high overall coverage, but the documentation and visibility are uneven (median 1.0; minimum 0.75). This suggests that some of the variation in staging reflects differences in the availability or shareability of governance artefacts rather than differences in whether governance occurs. Consequently, institutions that operate through informal practices may appear less mature in this domain because governance is not captured in documented instruments or formal structures.

Internal variation in Domain 3 is driven by differences in whether ICT governance is institutionalised through documented strategies with implementation roadmaps, broader and more coherent policy coverage, standing governance bodies with decision-making authority, and monitoring and review mechanisms that enable organisational learning. Baseline patterns indicate that many institutions have governance elements in place, but their visibility in formal artefacts, and the coherence and completeness of these elements, remain uneven across the system.

3.4.5 Implications for Institutions

Findings of Domain 3 imply that the differences in digital readiness among Somali HEIs are strongly influenced by the maturity of their governance – whether ICT is guided by formal instruments, supported by ongoing oversight and reinforced through monitoring and

review. The distribution of readiness stages suggests that governance remains a limiting factor for many institutions: only a few demonstrate “Relative Strength”, while the majority are categorised as “Developing” or flagged as a “Priority Area”.

Institutions without formal ICT strategies are likely to manage ICT development opportunistically. With 40% of institutions reporting no ICT strategy or master plan, decisions regarding ICT in these institutions are more likely to be driven by immediate operational pressures, procurement cycles or donor project requirements than by coherent sequencing and prioritisation. Even where strategies exist and have been approved, the absence of governance structures can limit follow-through and alignment across units.

Policy coverage gaps result in uneven controls and inconsistent institutional practice. While many institutions report at least one ICT-related policy, the median breadth of coverage is limited to just half of the assessed policy areas, with significant variation between institutions. Where documentation is limited or policies are narrow, institutions may face inconsistent practices across campuses and faculties, particularly with regard to procurement, service management, risk controls and emerging areas such as BYOD (Bring Your Own Device) and digital content governance.

The absence or weakness of steering committees reduces continuity and accountability. With fewer than one-third of institutions reporting formal ICT steering committees, oversight and prioritisation are likely to depend on informal executive channels or ad hoc decision-making. Even where committees do exist, they are often not sufficiently empowered, suggesting that the key institutional differentiator is not simply senior leadership involvement, but whether governance is structured in a way that creates continuity, cross-functional coordination and predictable decision-making processes.

Limited monitoring, auditing and reviewing practices constrain organisational learning. The low reporting of performance monitoring and formal

ICT audits indicate that many institutions lack systematic feedback loops to validate service delivery, identify weaknesses in controls or revise strategies and policies based on evidence. Consequently, institutions may continue to invest in ICT without having clear visibility of performance, user experience or risk exposure.

Domain 3 results imply that institutions will experience uneven returns from infrastructure and systems investments unless governance instruments are coherent, visible and reinforced by routine oversight and review. Those classified as “Relative Strength” are better placed to coordinate ICT decisions and manage risks across the institution, whereas “Developing” and “Priority Area” institutions are more likely to face fragmented implementation and limited accountability, even where individual policies or plans exist.

3.5 Core Digital Systems Availability

This domain evaluates the accessibility, implementation, and institutional integration of fundamental digital systems that support teaching, learning, research, and administration. The focus is on whether essential academic and administrative platforms are in place, how they are hosted, and how interconnected and used they are at an institutional level.

Key systems examined include student information systems, learning management systems, digital library platforms, research repositories, finance and enterprise systems, human resource systems, document management tools, video conferencing platforms, and plagiarism detection software. Indicators capture system type, platform choice, and hosting arrangements, distinguishing between locally hosted and cloud-based solutions.

The extent of interoperability between core platforms is used to assess system integration, including linkages between student information systems, learning management systems, library systems, finance systems, and human resource platforms. These indicators reflect the

extent to which digital systems operate as a coherent institutional ecosystem rather than as standalone applications.

The domain also considers system usage and functional coverage. Indicators capture the proportion of academic programmes using learning management systems, the range of academic and administrative processes that have been digitised and the ways in which users access institutional systems. These measures provide insight into whether systems are embedded in routine institutional operations.

Additionally, the assessment examines pedagogical integration and institutional support for digital teaching and learning. The indicators address the adoption of digital teaching practices, the availability of guidelines or incentives for ICT-enabled pedagogy, and the provision of support for faculty members, students, and digitally equipped teaching spaces.

Finally, the domain covers accessibility and inclusive design. The indicators assess the existence of institutional policies or guidelines on digital accessibility; the availability of accessibility features within digital platforms; whether accessibility assessments are conducted; and whether institutional responsibility for promoting inclusive digital practices is in place.

3.5.1 Baseline Conditions Across Somali HEIs

Digital systems are widely used to support core administrative functions across Somali HEIs, while the adoption of learning technologies and pedagogical approaches remains more uneven. Evidence suggests that digitisation has progressed further in student administration and enterprise functions than in learning platforms, system integration and inclusive digital teaching practices.

Table 19: Availability of core digital systems

Indicator	Summary
Student Information System (SIS) in use	96%
Learning Management System (LMS) in use	48%
Finance/ERP system in use	88%
Human Resources Information System (HRIS) in use	86%
Digital Library Management System in use	30%
Institutional digital repository in use	26%
Document Management System in use	40%
Video conferencing platforms in use	78%
Plagiarism detection software in use	26%
Average number of core digital systems per institution	5.2

Availability of core digital systems

Core administrative systems are widely reported. **96% of institutions report using a Student Information System (SIS)**, and enterprise systems are similarly prevalent, with finance/ERP systems (88%) and HRIS (86% each). Communication and collaboration platforms are also common, with 78% of institutions reporting the use of video conferencing platforms.

Learning and knowledge infrastructure is less consistently available. Fewer than half of institutions report using a Learning Management System (LMS) (48%). Systems that support academic content management and integrity, such as digital library management systems, institutional digital repositories, document management systems and plagiarism detection software, are reported by a minority of institutions. On average, institutions report using 5.2 core digital systems, reflecting a focus on a limited set of foundational platforms rather than a comprehensive digital ecosystem.

Reported system availability likely reflects a mix of different platforms, including commercial products, open-source solutions, bespoke databases and locally assembled tools. While this diversity enables incremental adoption, it also increases the burden on institutional ICT units to support interoperability, data governance, and user training.

System integration across institutional

platforms

Although evidence on system integration is limited, it is informative. Among institutions that use both an SIS (n=48) and an LMS (n=24), **58% reported integration between the two systems**, suggesting that some institutions have started to link learning and student administration workflows. However, integration indicators for finance, HR, SIS and library systems are not reported, indicating low integration maturity across the wider system.

Table 20: System integration across institutional platforms

Indicator	Summary
LMS and SIS integrated	58%
Finance and HR systems integrated	None
Finance and SIS integrated	None
Library systems and SIS integrated	None

The available evidence suggests that integration is progressing selectively, primarily where both systems are present and integration yields immediate operational benefits. Where systems are standalone or absent, integration is structurally constrained rather than a matter of institutional choice.

Integration feasibility is influenced by hosting and deployment models, including whether systems are vendor-hosted, locally hosted or part of integrated

enterprise suites. In the absence of systematic information on hosting arrangements, integration indicators should be interpreted as partial signals rather than comprehensive measures of interoperability.

Institutional usage and digitisation

The digitisation of core administrative processes is almost universal. 98% of institutions report having at least one core process that has been digitised. Specific functions are widely digitised, including course registration (94%) and student records or transcripts (98%), which is consistent with the near-universal use of Student Information Systems (SIS) platforms. Digitisation is also reported for staff recruitment and payroll (70%), with 58% of institutions reporting institution-wide capability for online exams and assessments. However, the assessment cannot distinguish between fully embedded use and more limited pilot

implementations.

Despite these strong signals of administrative digitisation, learning platform usage remains limited in scope. Among institutions that report using an LMS (n = 24), programme-level adoption varies widely:

- » 29% report LMS use in less than 25% of academic programmes.
- » 21% report use in 25–50% of programmes.
- » 17% report use in 51–75% of programmes.
- » 29% report usage in more than 75% of programmes.
- » 4% report that usage levels are unknown.

This distribution indicates that, even among institutions using an LMS, adoption is often uneven across faculties and programmes rather than being implemented institution-wide.

Table 21: Institutional usage and digitisation indicators

Indicator	Summary
Academic programmes using an LMS	Less than 25%
Institutions with at least one digitised core process	98%
Course registration digitised	94%
Student records or transcripts digitised	98%
Online exams or assessments in use	58%
Staff recruitment or payroll digitised	70%

The discrepancy between system availability and programme-level usage suggests that the adoption of pedagogical practices depends on factors beyond the mere presence of a platform, including staff capability, instructional design support, incentives and teaching norms. Informal tools, such as messaging platforms or shared drives, may substitute for formal LMS use, but they are not classified as structured learning technologies in this assessment.

Pedagogical and accessibility signals

There are limited formal mechanisms to support digital pedagogy. Only 25% of institutions report having ICT-in-

pedagogy guidelines or incentives, suggesting that institutional measures to encourage or standardise digital teaching practices are not yet widespread. Although teaching spaces are generally reported as being equipped with ICT tools, responses indicating “yes – widespread” are the most common, this perception-based indicator does not capture the consistency of equipment quality, maintenance or instructional support.

Accessibility-related governance shows partial uptake. 42% of institutions report having documented accessibility policies or guidelines, and 36% report having dedicated staff or a unit responsible for

digital accessibility. These figures suggest that a subset of institutions recognise accessibility considerations, but there is limited institutionalisation in terms of resourcing and operational ownership.

Table 22: Pedagogical and accessibility signals

Indicator	Summary
Institutions with ICT-in-pedagogy guidelines or incentives	24%
Teaching spaces equipped with ICT tools	Yes – widespread
Institutions with accessibility policies or guidelines	42%
Institutions with staff or unit responsible for digital accessibility	36%

Documented accessibility policies do not necessarily translate into accessible platforms or content. Effective accessibility depends on implementation practices, including accessible procurement requirements, platform configuration, staff training and the ongoing review of digital content and learning environments.

3.5.2 Readiness Indicators and Staging Logic

The availability of core digital systems is assessed using indicators that capture the presence, institutional deployment and integration of key academic and administrative platforms. These indicators are organised around four interrelated dimensions: system coverage; hosting and technical configuration; system usage and functional integration; and pedagogical and accessibility support.

Indicators of system coverage assess whether institutions have deployed essential digital platforms, such as student information systems, learning management systems, digital library systems, research repositories, finance and enterprise systems, human resource systems, document management tools and supporting platforms, including video conferencing and plagiarism detection software. These indicators establish the breadth of digital systems available to support institutional functions.

Hosting and configuration indicators determine whether systems are locally hosted or cloud-based, reflecting institutional approaches to scalability, maintenance, and security. While these indicators provide context on the technical environment in which digital platforms operate, they are not assessed in isolation from institutional capacity.

System usage and integration indicators examine the extent to which platforms are embedded in institutional operations. Examples include the proportion of academic programmes using learning management systems, the range of academic and administrative processes that have been digitised, and the degree of interoperability between core systems. This includes linkages between student information, learning management, library, finance, and human resource systems.

Pedagogical and accessibility indicators evaluate whether institutional practices promote the effective and inclusive use of digital systems. These indicators capture the presence of guidelines or incentives for ICT-enabled pedagogy; support mechanisms for faculty and students; the availability of ICT-equipped teaching spaces; and the inclusion of accessibility features within digital platforms. The existence of institutional responsibility for digital accessibility and the conduct of accessibility assessments is also considered.

The indicators in this category are considered together to determine the level of institutional readiness. These stages reflect the extent to which core digital systems are widely available, functionally integrated, actively used in teaching and administration, and supported by inclusive institutional practices. Depending on system coverage, integration, and support arrangements, institutions may occupy different readiness stages.

The staging logic is qualitative and comparative, informed by patterns across multiple indicators rather than mechanical scoring or weighted indices. This approach enables consistent interpretation across institutions while acknowledging variation in scale, system complexity, and implementation pathways.

3.5.3 Distribution of Readiness Stages Across Institutions

Domain 4 readiness stages summarise the range of core digital systems and learning platforms available at institutional level. These include administrative systems, learning and knowledge platforms, and the digitisation of selected core processes. The staging reflects the scope of the system landscape and institutional digital capacity rather than system integration, usage intensity or pedagogical effectiveness.

Distribution of readiness stages. For Domain 4, the distribution is

concentrated in the middle and upper stages, with meaningful differentiation across institutions. 52% of institutions (26) are classified as “Developing”, indicating that several core digital systems are in place, but there are gaps in the breadth or balance of systems across administrative and learning functions. A further 46% (23 institutions) are classified as “Relative Strength”, reflecting broader coverage of core systems and platforms. Only one institution (2%) is classified as a priority area, indicating that the availability of institutional digital systems is very limited relative to peers.

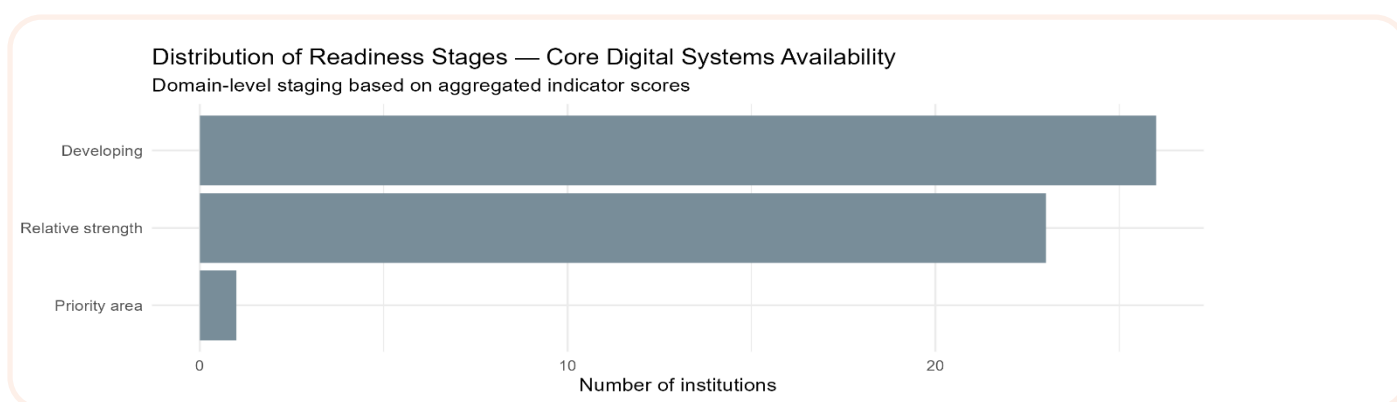


Figure 10: Distribution of readiness stages for digital systems and learning technologies

Evidence coverage for Domain 4 is uniformly high. The median domain coverage is 1.0, with no variation across institutions and all institutions reporting across the full indicator set. This suggests that the observed distribution reflects genuine differences in system scope, rather than missing data or inconsistent documentation.

Indicator breadth. Domain 4 comprises three indicators, with institutions reporting a median of three scored indicators and no observed variation in coverage. Therefore, differences in readiness stages are driven by variation in the number and mix of systems in use rather than incomplete reporting.

Interpreting Domain 4 stages.

01 Institutions classified as “**Relative Strength**” typically report multiple core administrative systems alongside learning and knowledge platforms. This indicates a broader

institutional digital landscape capable of supporting a range of academic and administrative functions.

02 In contrast, **Developing** institutions often report some key systems, such as a student information system or an enterprise platform, but lack coverage across the full set of core systems or learning platforms.

03 The small number of institutions flagged as a **Priority area** demonstrate very limited system availability, suggesting constrained institutional digital capacity.

As in other areas of this assessment, Domain 4 stages should not be taken as evidence of effective system integration, advanced pedagogical use or digital transformation outcomes. The assessment captures system presence and breadth, not interoperability, utilisation, or educational impact.

Link to baseline conditions. Domain 4 staging aligns with baseline findings showing high uptake of individual systems, such as SIS or finance platforms, alongside more limited adoption of learning platforms, digital repositories and document management systems. The predominance of the “Developing” category reflects the fact that system acquisition has often proceeded incrementally, resulting in uneven system landscapes across institutions.

System-level diagnostic implication. At this level, the results suggest that, while most Somali HEIs have moved beyond an absence of digital systems, system breadth and balance remain uneven. Strengthening the coherence and coverage of core digital systems, particularly learning and knowledge platforms, appears critical for enabling more advanced digital practices, including pedagogical innovation and data-driven institutional management.

3.5.4 Key Gaps and Internal Variations

The results for Domain 4 show a relatively mature baseline for administrative digitisation, alongside uneven uptake of learning technologies, limited integration across platforms and partial institutionalisation of pedagogical and accessibility support. The readiness stages are split between “Developing” (52%) and “Relative Strength” (46%), suggesting that, while most institutions have moved beyond a minimal systems environment, there is still variation in the breadth and balance of their digital ecosystems, particularly between administrative and academic functions.

While administrative systems are almost universal, learning and knowledge systems remain uneven. 96% of institutions report using a Student Information System (SIS), and 88% report using finance/ERP and HRIS systems (Table 19). By contrast, fewer than half of institutions report using an LMS (48%), and fewer than one-third report using a digital library management system (30%), an institutional repository (26%), or plagiarism detection tools (26%) (see Table 19). This creates a structural divide in system maturity: while most institutions

have digitised student administration and enterprise functions, fewer have institutional platforms to support learning delivery, academic content management and research knowledge infrastructure. Internal variation is therefore driven less by the presence of an SIS and more by whether institutions have layered learning and knowledge platforms on top of administrative systems.

System diversity is likely to increase the support burden and fragment institutional practice. The baseline notes that the reported systems comprise a variety of vendor products, open-source tools, bespoke databases and locally assembled solutions. While this diversity enables incremental adoption, it also increases demands on ICT units for configuration, maintenance, user training, and data consistency. Depending on how heterogeneous their platforms are and whether they can sustain them over time, institutions with similar “system counts” may differ substantially in operational complexity.

Integration remains narrow and selective, limiting end-to-end workflows. Among institutions with both an SIS and an LMS, only 58% report integration (see Table 20). Furthermore, integration indicators for finance–HR, finance–SIS and library–SIS are not reported, which suggests that interoperability is either weak or not systematically established across the broader platform landscape. Therefore, variation lies in whether institutions can connect student administration and learning delivery and whether institutional processes operate as linked workflows or as parallel systems with manual handoffs. Where systems are absent, integration is structurally constrained. Where systems exist but remain unintegrated, institutions face the challenges of duplicated data entry, inconsistent records and a limited ability to automate cross-functional processes.

Although the digitisation of administrative processes is widespread, it may mask the uneven depth of implementation. Almost all institutions (98%) report at least one digitised process, with course registration (94%) and student records/transcripts (98%) being almost universal (see Table 21). This aligns

with the high prevalence of SIS. However, other functions demonstrate weaker uptake, with online exams/assessments and staff recruitment/payroll achieving 58% and 70% respectively (Table 21). Furthermore, the assessment cannot distinguish between fully embedded institutional use and limited pilots. This introduces variation between institutions where digitisation is standard operating procedure and those where it exists but may be partial, unit-specific or dependent on a small number of staff.

The presence of a learning platform does not imply institution-wide use.

Among institutions that use an LMS (n = 24), the most frequently reported usage is “less than 25% of programmes”, and the distribution spans from minimal to widespread adoption. This indicates a common pattern within institutions: LMS adoption is often uneven across faculties and programmes rather than being consistently embedded institution-wide. Internal variation therefore exists not only between institutions with and without an LMS, but also within institutions that have an LMS but use it selectively. This suggests that platform adoption is shaped not only by platform availability, but also by staff capability, incentives, instructional design support and teaching norms.

The pedagogical support mechanisms available are limited and do not differentiate between institutions’ readiness beyond the presence of a system. Only 24% of institutions report having ICT-in-pedagogy guidelines or incentives (see Table 22). Even when teaching spaces are described as “equipped with ICT tools”, this is based on perception and does not take into account maintenance, suitability or the availability of instructional support. Consequently, institutions vary in their ability to provide a consistent digital teaching environment, which helps to explain why learning technologies lag behind administrative digitisation.

Accessibility governance is partial, with a discrepancy between policy signals and operational ownership. 42% of institutions report having documented accessibility policies or guidelines, and 36% report having staff or a unit responsible for digital accessibility (Table 22). This

suggests that accessibility is recognised by a subset of institutions, but ownership and resourcing are not yet widespread. There is likely to be substantial internal variation between institutions with formal responsibility for accessibility and those where it is addressed only through general ICT functions. There is also likely to be variation between institutions with policies and those with operational mechanisms to implement them.

Internal variation in Domain 4 is driven by differences in the balance of systems between administrative and learning/knowledge functions, the extent of interoperability between core platforms and whether learning technologies are adopted beyond isolated programmes. The baseline evidence suggests that, while many institutions have strong administrative digitisation foundations, the transition to coherent, integrated and pedagogically supported digital ecosystems remains uneven across Somali HEIs.

3.5.5 Implications for Institutions

Findings of Domain 4 imply that most Somali HEIs have moved beyond the absence of digital systems, with a high level of penetration of administrative platforms and the widespread digitisation of core student processes. The split between “Developing” (52%) and “Relative Strength” (46%) reflects differences in the breadth and balance of institutional platforms, particularly in terms of whether or not institutions extend beyond student administration and enterprise functions into learning and knowledge systems.

Institutions with core administrative systems but limited learning platforms are facing a structural ceiling on digital teaching. While near-universal SIS use and the high prevalence of finance/ERP and HRIS support transactional digitisation, the lower uptake of LMSs and knowledge systems suggests that digitisation of teaching and learning is not yet institution-wide in many cases. Even where an LMS exists, programme-level usage varies widely, implying that platform availability alone does not lead to consistent adoption across faculties.

Limited integration restricts end-to-end workflows and coherence of institutional data. Partial SIS–LMS integration among institutions with both systems indicates that some institutions are beginning to connect academic and administrative processes. However, broader interoperability across finance, HR, library, and document systems remains weak or is not yet established. Institutions with fragmented platforms are likely to rely on manual workarounds and duplicate data handling, resulting in inconsistent records and reducing the operational benefits of digitisation.

Beyond system counts, pedagogical support and accessibility ownership are key differentiators. With only 24% of institutions reporting ICT-in-pedagogy guidelines or incentives, it is clear that many are struggling to standardise digital teaching practice and sustain adoption. Similarly, documented accessibility policies and designated responsibility are lacking in many cases, suggesting that inclusive digital learning environments have not yet been institutionalised, even where systems exist.

Overall, Domain 4 results imply that institutional readiness increasingly depends on coherence and usage – whether platforms are integrated into workflows, adopted consistently in teaching and supported by enabling practices – rather than acquiring additional standalone systems. Institutions classified as “Relative Strength” are better positioned to support both administrative efficiency and learning delivery. However, “Developing” institutions risk remaining administratively digitised but pedagogically uneven, unless their platforms, usage, and support mechanisms mature together.

3.6 ICT Budgeting and Allocation

This domain evaluates how higher education institutions plan, allocate and maintain financial resources for ICT. It focuses on whether ICT investments are explicitly budgeted for, how costs are structured and financed, and the extent to which financial planning supports the long-term operation of digital systems.

The assessment looks at whether there are dedicated ICT budget lines and what proportion of institutional expenditure is allocated to ICT. Indicators capture what ICT budgets cover, including connectivity, hardware, software, staffing, maintenance and system upgrades. The assessment also considers whether institutions have developed or sustained core digital systems using internal resources rather than external or donor funding.

Funding sources are evaluated to determine the composition and stability of ICT financing. Indicators capture reliance on institutional revenues, student fees or service charges, donor or project funding, and other sources. The assessment also considers the use of cost-efficiency and cost-recovery strategies, including shared services, user fees or internal cross-subsidisation, where applicable.

The domain also examines financial governance and sustainability practices related to ICT. Indicators address whether ICT-specific procurement or financial approval guidelines are in place, and whether long-term sustainability considerations are integrated into institutional strategic or financial planning. Attention is given to institutional practices aimed at ensuring predictable funding for ongoing ICT operations, system renewal and future expansion.

Together, these indicators provide insight into whether ICT financing is treated as a recurring institutional obligation or an ad hoc or project-based expense, and whether financial arrangements support the sustained use and evolution of digital systems.

3.6.1 Baseline Conditions Across Somali HEIs

The financial arrangements for ICT in Somali HEIs are characterised by limited formalisation, narrow budget coverage and a heavy reliance on general institutional resources rather than diversified or self-sustaining funding models. While many institutions can estimate ICT costs informally, only a minority have dedicated ICT budget lines, and even fewer have comprehensive coverage of core ICT cost areas.

Table 23: ICT budget structures

Indicator	Summary
Institutions with a dedicated ICT budget line	34%
Institutions without a budget line but with an estimated ICT budget requirement	68%

ICT budget structures

Only 34% of surveyed institutions report having a dedicated ICT budget line as part of their formal financial structure. A further 68% report that they are nevertheless able to estimate ICT budget requirements informally, despite lacking a dedicated budget line. This suggests that, in many cases, ICT costs are visible to institutional management but are often embedded within broader operational budgets rather than being treated as a distinct category for planning and control.

The presence of a dedicated ICT budget line varies by institutional type. Dedicated ICT budgets are reported by one of eight public institutions, nine of 25 private institutions, one public-private partnership and six of 15 community-owned or foundation institutions. While these figures are not used for comparative assessment in this section, they do indicate an uneven institutionalisation of ICT financial planning across the system.

ICT budget coverage and scale

Among the institutions that reported having a dedicated ICT budget (n=17), the proportion of the total institutional budget allocated to ICT was most commonly reported to be in the **2–5% range**, based on banded responses. This suggests a relatively modest level of formal ICT investment, even among institutions that explicitly budget for ICT.

Budget coverage across ICT cost areas is partial. Only **34%** of institutions with a dedicated ICT budget report that it covers at least one core cost area comprehensively. Coverage varies by cost category: approximately one-third report coverage for **internet connectivity and bandwidth (32%)**, **hardware purchases and upgrades (34%)**, and **system maintenance and repairs (33%)**. Fewer

institutions report budget coverage for **software licences and subscriptions (28%)**, **ICT staff salaries and benefits (22%)**, **ICT training and professional development (25%)**, or **outsourced ICT services (21%)**.

Table 24: ICT budget coverage and scale (institutions with a dedicated ICT budget line)

Indicator	Summary
Proportion of institutional budget allocated to ICT	2 – 5%
Institutions whose ICT budget covers at least one core ICT cost area	34%
ICT budget covers internet connectivity and bandwidth	32%
ICT budget covers hardware purchase and upgrades	34%
ICT budget covers software licences and subscriptions	28%
ICT budget covers system maintenance and repairs	33%
ICT budget covers ICT staff salaries and benefits	22%
ICT budget covers ICT training and professional development	25%
ICT budget covers outsourced ICT services	21%

These patterns suggest that even when ICT budgets are in place, they frequently fail to cover the entire lifecycle of ICT costs, particularly those related to human capital, skills development, and long-term system sustainability.

ICT funding sources and cost recovery

Funding sources for ICT are limited in scope and diversity. Among institutions with a dedicated ICT budget, only **36%** report having at least one clearly identified ICT funding source besides ad hoc allocations. Where funding sources are identified, institutions primarily relied on the **core institutional budget (36%)**, with minimal use of **donor or project-based funding (5%)**, **student technology or service fees (2%)**, **government or agency subsidies (2%)**, or **research grants or projects (2%)**. No institutions report revenue-generating ICT services as a funding source.

Cost-efficiency and recovery strategies are rare. Only 8% of institutions with a dedicated ICT budget report using any such mechanisms as shared procurement, bandwidth optimisation, cost-sharing arrangements with partners (including SomaliREN), internal expenditure monitoring or charging for selected ICT services.

Table 25: ICT funding sources and cost recovery mechanisms (institutions with a dedicated ICT budget line)

Indicator	Proportion
Institutions with at least one identified ICT funding source	36%
Institutional core budget	36%
Donor or project-based funding	5%
Student technology or service fees	2%
Revenue-generating ICT services	0%
Government or agency subsidies	2%
Research grants or projects	2%
Institutions using any ICT cost-efficiency or recovery strategy	8%

The limited uptake of diversified funding sources and cost-recovery strategies suggests that ICT sustainability remains largely dependent on general institutional finances. Where alternative mechanisms exist, they appear to be isolated rather than systematised across institutions.

Financial governance and sustainability signals

Financial governance arrangements show mixed maturity. Among institutions with a dedicated ICT budget, 63% report having ICT-specific procurement or financial approval guidelines, indicating some level of control over ICT-related expenditure. However, only 32% report that ICT sustainability considerations are explicitly incorporated into planning and budgeting processes.

Table 26: Financial governance and sustainability signals (institutions with a dedicated ICT budget)

Indicator	Summary
Institutions with ICT-specific procurement or financial approval guidelines	63%
Institutions that explicitly consider ICT sustainability in planning	32%

Explicit consideration of ICT sustainability remains limited. In many institutions, ICT budgeting appears to focus on short-term operational needs rather than lifecycle costing, replacement planning or long-term affordability. This restricts the capacity to maintain and expand digital systems as institutional reliance on ICT continues to increase.

The prevalence of informal ICT budgeting and narrow cost coverage is consistent with the reported reliance on internally developed or locally adapted systems in other areas. While such approaches can reduce initial costs, they often result in ongoing financial pressures relating to maintenance, staff time and ad hoc upgrades, which are not consistently accounted for in formal ICT budgets.

3.6.2 Readiness Indicators and Staging Logic

Readiness in ICT budgeting and allocation is assessed using indicators that measure the visibility, adequacy and sustainability of financial resources for ICT. These indicators are organised into four interrelated categories: budget structure; funding sources; cost management practices; and long-term financial planning.

Budget structure indicators assess whether institutions have dedicated ICT budget lines, as well as the proportion of institutional expenditure allocated to ICT. They also capture the scope of ICT expenditure, including connectivity, hardware, software, staffing, maintenance and system upgrades, as well as the extent to which institutions finance core digital systems with internal funds.

Funding source indicators examine the composition and stability of ICT financing. Reliance on institutional revenues, student fees or service charges, donor or project-based funding, and other sources is considered. These indicators provide insight into the predictability of ICT funding and the exposure to short-term or external financing.

Cost management indicators evaluate the implementation of cost-efficiency or cost-recovery strategies, such as shared services, internal cross-subsidisation, or user-based charges. The presence of ICT-specific procurement or financial approval guidelines is also considered, reflecting the institutional capacity to manage ICT expenditure systematically.

Long-term planning indicators examine whether the sustainability of ICT systems is explicitly considered in institutional strategic or financial planning. The presence of practices aimed at ensuring ongoing funding for system operation, renewal and expansion rather than one-off investments is also captured by the indicators.

The indicators within this domain are considered together to describe institutional conditions across a small number of readiness stages. These stages reflect the extent to which ICT financing is predictable, adequately planned and aligned with institutional priorities. Depending on the balance between budget formalisation, funding stability, cost management practices, and long-term sustainability planning, institutions may occupy different readiness stages.

The staging logic is qualitative and comparative, informed by patterns across multiple indicators rather than mechanical scoring or weighted indices. This approach enables consistent interpretation across institutions while acknowledging variation in size, financial capacity and funding models.

3.6.3 Distribution of Readiness Stages Across Institutions

The Domain 5 readiness stages summarise the extent to which institutions demonstrate the basic financial foundations necessary for ICT sustainability. This includes the recognition of ICT costs through a budget line or structured estimation, identification of ICT funding sources and the presence of governance signals that support planned, cost-effective ICT operations. The staging reflects financial structuring and institutionalisation rather than the adequacy of ICT budgets, affordability or the long-term viability of financing.

Distribution of readiness stages. The distribution indicates that, while most institutions have some elements of ICT budgeting and financial planning in place, stronger institutionalised arrangements are less common. The majority of institutions (54%, or 27 institutions) are classified as “Developing”, which suggests partial financial structuring, typically characterised by some budget recognition and limited governance signals, but incomplete mechanisms for funding diversification and sustainability. Approximately one-third (32%, or 16 institutions) are classified as “Relative Strength”, indicating a comparatively stronger combination of budgeting commitment, diversified funding signals and/or more established governance mechanisms. A smaller subset (14%, or seven institutions) are flagged as a priority area, reflecting limited evidence of structured ICT budgeting or sustainability governance compared to their peers.

Distribution of Readiness Stages — ICT Budgeting and Allocation
Domain-level staging based on aggregated indicator scores

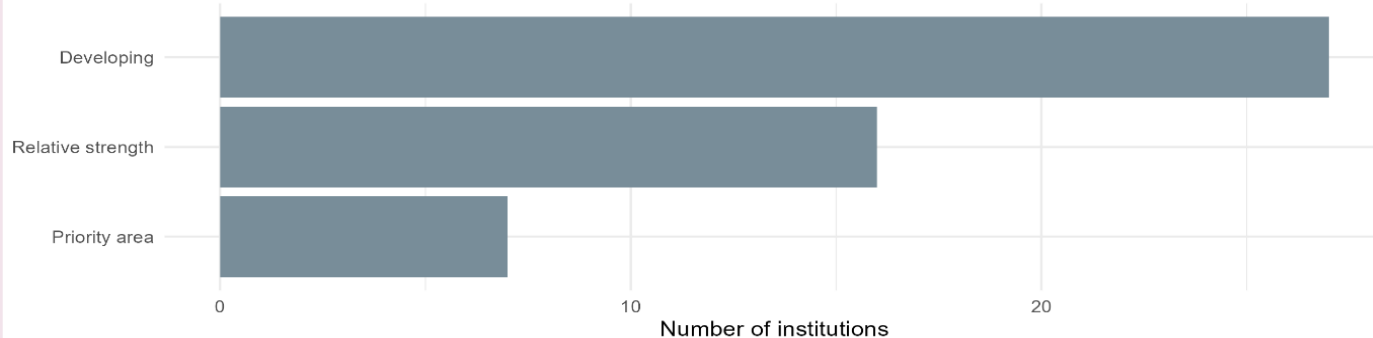


Figure 11: Distribution of readiness stages for financial sustainability

Evidence coverage and staging confidence. Evidence coverage for Domain 5 is uneven. The median domain coverage is 0.33, with a wide interquartile range of 0.67 and an observed minimum coverage of 0.17. This suggests that many institutions only provided evidence for a subset of the financial sustainability indicators. The staging therefore captures both genuine variation in financial sustainability arrangements and limited documentation and visibility of budgeting, funding and governance practices. Consequently, Domain 5 classifications should be interpreted as conservative indicators of financial structuring rather than definitive measures of financial capacity.

Indicator breadth. The domain comprises six indicators, but institutions report a median of two scored indicators, with substantial dispersion (IQR 4) and a minimum of one scored indicator. This pattern suggests that financial sustainability evidence is often concentrated in a small number of areas, rather than being represented by a comprehensive set of budgeting, funding and governance mechanisms. Differences in readiness stages are therefore driven by variation in:

- » Whether ICT is recognised within budgeting processes
- » Whether institutions can identify more than one ICT funding source
- » Whether any sustainability governance mechanisms are evident.

Interpreting Domain 5 stages:

- 01 Institutions classified as “Relative Strength” tend to demonstrate clearer evidence of ICT budgeting commitment (e.g. a defined budget line rather than informal estimates), as well as signals of funding source breadth and/or the presence of governance mechanisms that support procurement, sustainability planning or cost-efficiency approaches.
- 02 In contrast, developing institutions typically demonstrate early-stage financial structuring, often showing at least one budgeting signal and limited evidence of governance mechanisms, but with narrow funding models and incomplete sustainability planning.
- 03 Institutions flagged as a priority area generally demonstrate limited evidence across the available indicators. This suggests that their ICT budgeting and sustainability mechanisms are less well-established than those of their peers.

Domain 5 staging does not assess whether ICT allocations are sufficient to meet institutional needs, nor does it capture the predictability of funding flows or the effectiveness of expenditure management. Rather, it provides a structured view of whether the financial building blocks for sustaining ICT operations are evident in institutional practice and documentation.

System-level diagnostic implications.

At a system level, the results indicate that ICT financial sustainability remains a constraint on digital transformation across Somali HEIs. While many institutions demonstrate partial budgeting and planning, evidence of comprehensive, institutionalised financing mechanisms is less widespread. Inconsistent documentation and limited indicator coverage suggest that, while financial sustainability practices may exist, they are not consistently formalised, tracked or communicated in a way that supports strategic ICT investment and long-term system reliability.

3.6.4 Key Gaps and Internal Variations

The financial sustainability signals in Domain 5 demonstrate significant variation in the way institutions recognise, structure and document ICT financing. The baseline findings suggest that, while most institutions can articulate ICT needs informally, fewer translate this into formal budgeting instruments, lifecycle coverage or sustainability-oriented governance. The staging results reinforce the idea that this variation is driven by uneven documentation and indicator coverage as well as underlying financial practice.

There are gaps in budget recognition and formalisation. Only one-third of institutions (34%) report a dedicated ICT budget line, while a much larger proportion (68%) of those without a budget line report an informal ability to estimate ICT needs. This suggests a common pattern whereby ICT expenditure is anticipated, but not consistently ring-fenced, which limits traceability and internal accountability for ICT spending. Further analysis reveals that budget line institutionalisation varies across different types of institution. Public institutions are the least likely to report a dedicated line (1 in 8), while private and community-owned/foundation institutions demonstrate higher, albeit still partial, adoption. These differences point to divergent budgeting practices and governance norms rather than uniform, sector-wide approaches.

There is narrow and uneven coverage of ICT cost areas. Among institutions

with a dedicated ICT budget (n = 17), reported coverage of core cost categories is fragmented. Around one-third report covering connectivity, hardware and maintenance (32–34%), but coverage is notably weaker for recurrent and capacity-related costs, such as staff salaries (22%) and training (25%), as well as outsourced services (21%). Even within the subgroup that explicitly budgets for ICT, this pattern suggests substantial internal variation in whether budgets address full operational needs or focus on visible infrastructure items. The result is an uneven ability to sustain systems beyond initial procurement, especially given that platform maintenance, licensing, security controls and staff capability development require ongoing funding.

There is low funding diversification and minimal cost recovery. Funding sources beyond the institutional core budget are rarely reported. Among institutions with dedicated ICT budgets, only 36% report at least one identified ICT funding source. Where sources are specified, reliance is overwhelmingly on the institutional core budget (36%). Donor funding (5%), student fees (2%), subsidies (2%) and research grants (2%) appear to play a marginal role, with no institutions reporting revenue-generating ICT services. The low prevalence of cost-efficiency or recovery strategies (8%) suggests that most institutions have limited means of stabilising ICT financing, particularly for recurring costs. There is variation not only between institutions, but also within institutions: some apply informal cost controls or ad hoc service charges, but these are neither widely formalised nor visible as part of an institutional financing model.

Although governance signals exist, sustainability intent is limited. While 63% of institutions with a dedicated ICT budget report procurement or approval guidelines for ICT, indicating that some controls over ICT expenditure exist, only 32% report that ICT sustainability is explicitly considered in planning. This suggests a governance gap between transactional controls (approving purchases) and strategic financial management (planning for renewal cycles, ongoing operating costs and long-term affordability). Institutions

differ in where they sit on this spectrum: some have formal procurement controls without associated sustainability planning, while a smaller subset appear to have both.

Evidence gaps and visibility constraints shape the observed variation. Domain 5 has the lowest and most uneven evidence coverage (median coverage 0.33; minimum 0.17) and institutions report a median of two out of six scored indicators. This implies that internal variation is partly driven by the limited documentation and visibility of financial practices rather than by the absence of activity. In several institutions, ICT financing may occur through consolidated administrative budgets, donor-funded projects or informal allocations, which are difficult for respondents to categorise. Consequently, gaps in Domain 5 should be interpreted as “limited structuring and visibility of ICT financial mechanisms” rather than definitive absence of ICT spending.

The key variation among Somali HEIs is between those that can demonstrate a basic budgeting instrument and some governance controls, and those where ICT financing remains largely informal and difficult to evidence across lifecycle cost categories. The most common system pattern is partial budgeting recognition without a consistent funding model, full cost coverage or sustainability-oriented planning.

3.6.5 Implications for Institutions

Findings of Domain 5 suggest that, while many Somali HEIs recognise ICT as a cost driver, fewer can demonstrate institutionalised financial mechanisms that support reliable operations and long-term system sustainability. The most common pattern is informal budgeting visibility without consistent formal allocation, lifecycle coverage or defined funding models.

For institutions without a dedicated ICT budget, allocating funds to ICT is likely to remain challenging within internal budgeting cycles, especially when these costs are embedded within broader operational lines. Even when institutions can estimate their ICT needs informally,

the absence of a formal budget structure means that managers have little clarity over what is funded, what is deferred, and how ICT commitments relate to institutional goals.

Among institutions with a dedicated ICT budget (n = 17), reported budget coverage across core cost areas is partial and often infrastructure-weighted. Limited coverage of recurrent costs, such as ICT staffing, training, software licences and outsourced services, signals vulnerability in terms of operational continuity and skills development, particularly as reliance on digital systems increases. Consequently, system availability may coexist with underfunded maintenance, patching, support capacity and renewal cycles.

The narrow reporting of diversified funding sources and limited uptake of cost-efficiency or recovery strategies across the system indicate that most institutions remain dependent on core resources. This increases their exposure to short-term budgetary pressures and reduces their flexibility to sustain digital platforms as requirements expand, including those relating to security, data protection and learning technologies.

Finally, the uneven coverage of evidence in this area implies that some institutions may have informal or hidden financial practices. From an institutional readiness perspective, however, limited documentation and weak internal visibility are constraints in themselves because they reduce the ability to plan, coordinate and govern ICT investment coherently over time.

3.7 System and Network Security

This domain evaluates the practices of higher education institutions for safeguarding ICT infrastructure, protecting data and managing digital risks. It examines whether higher education institutions have the necessary technical controls, organisational responsibilities and procedural arrangements to protect digital systems and ensure business continuity.

The assessment looks at how aware institutions are of cybersecurity and data protection standards, how compliant they are with these standards, and whether responsibility for ICT security is formally assigned to a designated unit or role. These indicators reflect the extent to which security is recognised as an institutional function rather than an ad hoc technical task.

Technical security measures are evaluated using indicators that cover user account and access management, the implementation of security controls, and the protection of servers and ICT equipment. Practices related to authentication, access privileges, and the physical security of critical ICT infrastructure are also considered.

Data protection and continuity are examined through institutional practices for data backup and recovery. The indicators capture information on whether data backups are conducted, the types of data covered, the level of automation, storage arrangements and whether backup restoration or disaster recovery processes are periodically tested.

The domain also considers institutional approaches to risk management and incident response. Indicators assess whether formal ICT risk assessments have been conducted and whether institutions have experienced recent security incidents. They also assess the existence of incident response plans or protocols. Together, these measures provide insight into institutional preparedness to prevent, detect and respond to digital security threats.

3.7.1 Baseline Conditions Across Somali HEIs

Institutional arrangements for data security and risk management reveal a combination of fundamental practices and substantial shortcomings in terms of formal accountability, layered controls and tested response mechanisms. While about half of institutions report awareness of cybersecurity and data protection issues, formal accountability structures and systematic risk management practices are less consistently in place.

Table 27: Security responsibility and awareness

Indicator	Summary
Institutions aware of and compliant with cybersecurity or data protection standards	50%
Institutions with formally assigned ICT security responsibility	44%

Security responsibility and awareness

Only 50% of institutions report being aware of cybersecurity or data protection standards, based on self-reported awareness rather than verified compliance. Formal assignment of responsibility for ICT security is reported by 44% of institutions (22 out of 50), indicating that accountability for security is informal or implicit within general ICT roles in the majority of institutions.

This discrepancy between awareness and formal responsibility suggests that, while security considerations are present at a conceptual level in many institutions, they are not consistently embedded in organisational structures or job roles.

Core security and access controls

Among institutions that report having formally assigned ICT security responsibility, 44% have at least one technical security measure in place. The most commonly reported controls are secured Wi-Fi access (42%), internal network segmentation (26%), and antivirus or malware protection (36%). More advanced perimeter controls are less common: only 18% report perimeter firewalls or intrusion prevention systems and 26% report access controls for sensitive systems. Regular updating and patching of operating systems and software is reported by 36% of institutions in this group.

Table 28: Core security and access controls

Indicator	Summary
Institutions with at least one technical security measure in place	44%
Perimeter firewalls or intrusion prevention systems in place	18%
Internal network segmentation implemented	26%
Wi-Fi access secured	42%
Antivirus or malware protection deployed	36%
Access controls for sensitive systems implemented	26%
Operating systems and software regularly updated or patched	36%
Institutions with structured user account or access management practices	98%

These figures suggest that, where security responsibility exists, controls are frequently implemented selectively rather than forming part of a layered security architecture. Therefore, the presence of individual measures should not be interpreted as providing comprehensive protection.

User account and access management practices are reported more widely. 98% of institutions report having some form of structured user account or access management. However, these practices vary widely, ranging from password policies and centralised user management systems to manual or ad hoc account handling. This suggests that, although basic account provisioning is widespread, the maturity of access governance varies substantially across institutions.

Data protection and backup practices

Data backup practices are widely reported. 94% of institutions indicate that they back up institutional data, with “regularly” being the most common response. Backup processes are most commonly described as automated, though some institutions report manual or mixed approaches.

Despite the prevalence of backup practices, recovery assurance is less consistent. Only 47% of institutions

report having tested data restoration or disaster recovery processes within the past 12 months. This suggests that many institutions may not have verified their ability to restore data following an incident.

The provision of cybersecurity or data protection training to ICT staff is reported by 41% of institutions, suggesting that capacity building in security practices is present in some institutions, but not yet widespread.

Table 29: 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%

Reported backup practices do not provide visibility into backup scope, storage location, redundancy or retention policies. Automated backups may still be vulnerable if they are stored on-site without off-site replication, or if restoration procedures are not routinely tested.

Incident experience and risk management signals

Formal risk management practices remain limited. **Only 18% institutions report having conducted a formal ICT risk assessment in the past three years.** Of these, two-thirds reported having an incident response plan in place, while the remaining third indicate that a plan is under development.

Reported incident experience indicates that operational disruptions are common. **52% of the institutions reported system downtime** due to power or hardware failure in the past two years, and 48% reported internet outages lasting more than one day. Security-related incidents

are reported less frequently but are still significant: one quarter of institutions (24%) report attempted or successful cyberattacks; 16% reported data loss or corruption; and 2% reported a breach of student or staff data.

These patterns suggest that, although severe data breaches are rare, service disruptions and security incidents are an ongoing operational issue, highlighting the importance of preventive measures and tested response mechanisms.

Physical security conditions

The physical protection of ICT infrastructure varies widely. 42% of institutions reported some form of access control for server or ICT equipment rooms, while 36% reported backup power systems, 30% reported cooling or ventilation systems and 22% reported fire detection or suppression systems. **Conversely, half of the institutions (52%) report having none of these physical security measures in place.**

The absence of basic physical safeguards in a substantial number of institutions increases the risk of equipment damage, unauthorised access and service interruption, particularly in environments with unreliable power supplies and limited environmental controls.

3.7.2 Readiness Indicators and Staging Logic

Readiness in terms of system and network security is assessed using indicators that measure the presence, consistency and institutionalisation of measures designed to protect ICT infrastructure, data and digital services. These indicators are organised into four interrelated categories: security governance and responsibility; technical security controls; data protection and continuity; and risk management and incident response.

Security governance indicators evaluate whether responsibility for ICT security has been formally assigned to a specific department or position, and whether institutions are familiar with, or adhere to, relevant cybersecurity and data protection standards. These indicators reflect the extent to which security is treated as an

institutional responsibility rather than an ad hoc technical function.

Technical security control indicators examine practices for managing user accounts and access, implementing security measures, and protecting servers and ICT equipment. Attention is given to authentication practices, access privileges, and physical safeguards for critical ICT infrastructure.

Data protection and continuity indicators evaluate institutional practices for data backup and recovery. This includes determining whether data backups are conducted, the types of data covered, the level of automation, storage arrangements and whether disaster recovery or backup restoration processes are tested periodically.

Risk management and incident response indicators capture whether institutions conduct formal ICT risk assessments, have experienced security incidents and maintain incident response plans or protocols. These practices are considered to be indicators of an institution's preparedness to anticipate, manage and respond to digital security threats.

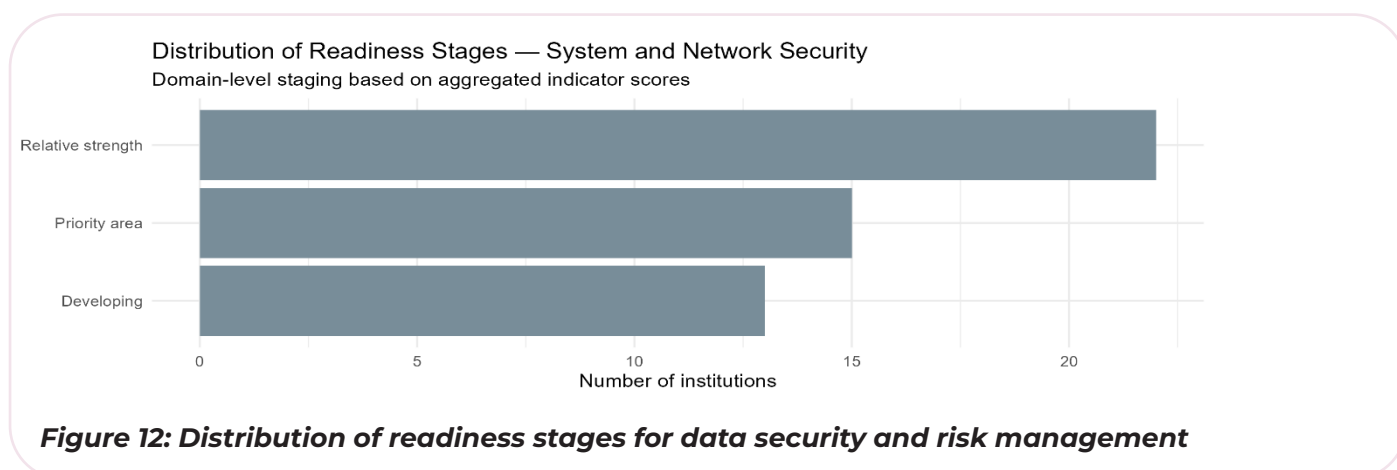
The indicators within this domain are interpreted collectively in order to characterise institutional conditions in relation to a small number of readiness stages. These stages reflect the extent to which security practices are formalised and consistently implemented within institutional operations. Depending on the balance between governance arrangements, technical controls, data protection practices, and risk management capabilities, institutions may occupy different readiness stages.

The staging logic is qualitative and comparative, informed by patterns across multiple indicators rather than mechanical scoring or weighted indices. This approach enables consistent interpretation across institutions while acknowledging variation in scale, risk exposure and resource constraints.

3.7.3 Distribution of Readiness Stages Across Institutions

The Domain 6 readiness stages assess the extent to which institutions demonstrate ownership of basic security measures and layered safeguards for protecting their systems and data. The staging is based on composite indicators covering security awareness and assignment of responsibility; technical, physical and access control measures; backup and recovery practices and risk recognition and incident management signals. The results should be interpreted as conservative indications of the presence and depth of the practices rather than as verified evidence of the effectiveness of the controls or compliance with any external standard.

Distribution of readiness stages. The distribution suggests a mixed security posture across Somali HEIs, with a substantial proportion showing limited evidence of foundational security practices. A comparatively stronger combination of security responsibility and layered measures is observed in 44% of institutions (22/50). Conversely, 30% (15/50) are categorised as a priority area, reflecting weaker or less comprehensive visibility of security ownership, controls, and risk management signals compared to their peers. The remaining 26% (13/50) are classified as “Developing”, suggesting the partial adoption of security measures, often with some basic safeguards present but with limited depth, inconsistent layering or uneven operationalisation.



Evidence coverage and staging confidence. Evidence coverage for Domain 6 is moderate and uneven. The median domain coverage is 0.50 (IQR 0.25), with a minimum observed coverage of 0.25. This suggests that many institutions only provided evidence for part of the domain, which limits the confidence with which strong conclusions can be drawn in some cases. The staging therefore reflects genuine variation in security posture, as well as limited documentation and visibility for certain security and risk management components. In this context, “Priority area” classifications should be interpreted as indicating limited or incomplete evidence of foundational security practices, rather than as proof of their absence.

Indicator breadth. The domain comprises four indicators, but institutions report a median of two scored indicators (IQR 1;

minimum 1). This suggests that security maturity is typically evidenced through a limited subset of signals, rather than being demonstrated consistently across the entire chain, from ownership to controls, resilience, and response. Consistent with this, domain scores cluster at discrete values that reflect partial adoption. Ten institutions score 0.0, indicating no reliable evidence across the scored indicators; five institutions score 0.33, reflecting isolated measures without layering; and eleven institutions score 0.5, indicating that two out of four capability areas are evidenced. Only a small number of institutions achieve higher composite scores (e.g. 0.89 for three institutions), which is consistent with security maturity being relatively rare and requiring multiple reinforcing elements.

- 01 Institutions classified as **“Relative Strength”** typically demonstrate clearer evidence of formal responsibility for ICT security, combined with multiple layers of safeguards, such as technical controls, physical protections, structured access management practices and more mature backup arrangements, including automation and/or testing.
- 02 **Developing** institutions generally demonstrate partial adoption, often reporting at least one or two security elements (e.g. backups and basic access management), but with limited evidence of consistent layering across the technical, physical, recovery and incident response dimensions.
- 03 Institutions flagged as a **Priority area** tend to show limited or fragmented evidence across the domain. This includes weak visibility of responsibility assignment, limited controls beyond baseline practices and minimal signals of risk assessment or incident management mechanisms.

Domain 6 staging does not evaluate the effectiveness of safeguards, configuration quality, or adherence to formal cybersecurity frameworks. Rather, it provides a system-level view of whether key security building blocks are visible and sufficiently layered to support reliable digital operations.

System-level diagnostic implication. At this level, the results suggest that security and risk management are essential for digital transformation in Somali HEIs. While a subset of institutions report relatively stronger practices, the overall pattern reveals uneven security maturity and limited visibility of controls, resilience practices and incident management mechanisms within many institutions. This has implications for the reliability of digital service delivery and the safe expansion of institutional systems, particularly as institutions increase their use of interconnected platforms and data-driven services.

3.7.4 Key Gaps and Internal Variations

Findings of Domain 6 reveal significant discrepancies between the implementation of fundamental security measures and the establishment of thorough, multi-layered security and risk management systems. Although many institutions report the implementation of individual security measures, these are distributed unevenly across governance, technical controls, resilience, and response capabilities.

The level of security maturity in Somali HEIs is uneven because formal accountability, layered controls, tested recovery and risk-response mechanisms are not consistently present together. Baseline evidence indicates a discrepancy between reported awareness and institutional ownership: although 50% of institutions report awareness of cybersecurity or data protection standards, only 44% (22 out of 50) formally assign ICT security responsibility to a specific unit or role. This discrepancy creates clear internal variation – some institutions can anchor security in defined roles, while many rely on implicit responsibility within general ICT functions.

There are accountability and governance gaps. The 6 percentage-point gap between awareness (50%) and formally assigned responsibility (44%) suggests that, while security is generally understood, it is not consistently institutionalised. This affects how security priorities are set, resourced and sustained over time. It also helps to explain why stronger security postures are found in only a subset of institutions: in the staging results, 44% (22/50) fall into the “Relative Strength” category, which closely mirrors the proportion that report formal security responsibility. Meanwhile, 30% (15/50) are flagged as a “Priority Area”, reflecting limited visibility of foundational ownership and controls.

Safeguards are implemented in a partial and selective manner. Where formal security responsibility exists, the reported controls are often found in isolated pockets rather than forming a coherent, layered security architecture. Only 18% of organisations report having perimeter firewalls or intrusion prevention systems,

26% report having internal network segmentation and 26% report having access controls for sensitive systems. Basic protections are more common, but still not universal: secured Wi-Fi (42%), antivirus/malware protection (36%), and regular updating/patching (36%). In contrast, 98% report some form of structured user account or access management, yet this ranges from password policies and centralised user management to manual or ad hoc practices. This means that “presence” does not imply consistent maturity. This uneven mix produces wide variation in effective protection, even among institutions that report at least one control.

Resilience practices are common, but assurance is weaker. Data backup is widely reported (94%), with “regularly” being the most common backup frequency and “automated” being the most common backup mode. However, only 47% report having tested disaster recovery or backup restoration in the last 12 months. This creates a pronounced split between institutions that have validated recoverability and those where continuity is merely assumed. Training in cybersecurity or data protection for ICT staff is also inconsistent (41%), which reinforces differences in the ability to maintain and improve controls over time.

Despite frequent disruptions, risk recognition and response remain limited. Only 18% of respondents reported conducting a formal ICT risk assessment in the past three years. Of those who did (n = 9), two-thirds (6/9) report having an incident response plan in place, while one-third (3/9) report having a plan under development. This suggests that the capacity for incident response is concentrated within a very small subset of institutions. At the same time, operational disruption is commonplace: 52% of respondents reported system downtime due to power or hardware failure, while 48% reported an internet outage lasting more than one day within the past two years. Security incidents are less frequent, but still significant: attempted/successful cyberattacks (24%), data loss/corruption (16%), and breach of staff/student data (2%). Therefore, the variation is not only in exposure, but also in whether institutions

have formal mechanisms to anticipate and respond.

Physical security is a major differentiator. Physical protections are uneven, with many institutions reporting no basic safeguards. While 42% report access control for server or ICT equipment rooms, only 36% report backup power, 30% report cooling or ventilation, and 22% report fire detection or suppression. Half of institutions (52%) report none of these measures. This results in significant differences in vulnerability to theft, damage, overheating, and outage-driven equipment failure, which has direct implications for reliability and security continuity.

Evidence gaps influence the observed variation and staging confidence. Domain 6 has moderate and uneven evidence coverage (median 0.50, IQR 0.25, minimum 0.25), and institutions report a median of two out of four scored indicators (IQR 1, minimum 1). Domain scores cluster at discrete values, which are consistent with partial adoption: Ten institutions score 0.0, five score 0.33, eleven score 0.5, and nineteen score 1.0. This suggests that internal variation reflects genuine differences in security posture as well as uneven visibility and documentation of controls, particularly with regard to risk assessment and incident response.

Key internal variations across Somali HEIs are evident between a minority of institutions that combine assigned responsibility, multiple layers of safeguards and some assurance practices (testing and review), and a larger group where security is present in the form of basic or isolated practices (notably backups and account provisioning), but lacks consistent layering, physical protection and formal risk-response mechanisms.

3.7.5 Implications for Institutions

The security readiness of Somali HEIs depends less on the existence of any single control and more on their ability to demonstrate ownership, layered safeguards, tested recovery and basic risk-response routines as an integrated practice. The baseline and staging results show that, while many institutions have

elements of security in place, notably backups and account management, fewer have the combination required to protect institutional systems as digital dependence grows.

With only 44% (22/50) of institutions reporting that ICT security responsibility has been formally assigned – despite 50% reporting awareness – institutions should prioritise clearly assigning roles, authority and minimum security duties within the ICT function (or an equivalent unit). Where responsibility is not formalised, security improvements tend to be ad hoc and difficult to sustain.

Reported safeguards are uneven. Institutions should adopt a small, staged baseline combining secured Wi-Fi, endpoint protection, patching routines, basic segmentation for sensitive systems and controlled access for core platforms. This approach enables institutions with limited resources to develop robust coverage without attempting to implement “best practice” architectures immediately.

Although 94% of people report that they back up their data, and automation is commonly reported, only 47% have tested restoration or disaster recovery in the last 12 months. Institutions should implement routine restoration tests, define recovery roles and ensure that backups are protected against the same risks that affect primary systems, such as power failure, theft, ransomware and physical damage. Without testing, backup practices provide limited assurance.

The high proportion reporting no physical protection (52%), alongside the low prevalence of backup power (36%), cooling and ventilation (30%), and fire suppression (22%), means that many institutions remain exposed to preventable failures and service disruption. Improving server room access control and power and environmental protection is often a cost-effective way to reduce downtime and security incidents.

Only 18% have conducted a formal ICT

risk assessment in the past three years, and incident response planning is concentrated within this small group. Yet operational disruption is commonplace, with 52% reporting downtime due to power or hardware failure, 48% reporting internet outages of more than one day and 24% reporting cyberattacks. Institutions should adopt lightweight annual risk reviews, maintain an incident log and implement a simple incident response protocol covering escalation, containment, communication and recovery.

Interpret “priority area” as a call for minimum baseline standards and documentation. As 30% of institutions have been identified as a priority area and domain coverage is only moderate (median 0.50), institutions should improve the visibility and documentation of existing practices (e.g. responsibility assignment, policies/protocols, audit/testing records). This will improve governance confidence and enable institutions to plan improvements systematically rather than relying on the informal knowledge of ICT teams.

4 National Readiness Synthesis and Typologies

This chapter summarises the findings from the different domains presented earlier to provide a national overview of digital readiness in higher education in Somalia. Rather than revisiting individual indicators or institutional results, it focuses on how readiness patterns emerge and vary across domains and institutions at a system level. Readiness tiers are used as the primary summary lens to indicate how far institutions have progressed overall, while typologies are applied within tiers to explain how digital readiness is configured in practice across key domains. The analysis is intentionally anonymised and interpretive, drawing on a limited but systematic quantitative evidence base to highlight structural patterns, internal variation and recurring bottlenecks, rather than ranking institutions or implying normative benchmarks.

4.1 Aggregate Readiness Patterns Across Domains

This section provides a national overview of digital readiness in Somali HEIs, synthesising results from different domains. It establishes the broad configuration of strengths, gaps and internal variation across domains before introducing readiness tiers and within-tier typologies as organising lenses in subsequent sections.

4.1.1 Cross-domain readiness distribution

Figure 13 summarises the distribution of readiness stages across the six assessed domains, using flags to distinguish between “relative strength”, “developing”, “priority area” and “insufficient data”. Including the latter reflects the application of minimum evidence thresholds at the domain level. This allows the analysis to differentiate between demonstrated performance and areas where there is insufficient data to support a robust classification.

The results continue to reveal an asymmetry between domains associated with operational provision and those linked to institutionalisation, governance and risk management, though important refinements have emerged. Infrastructure and connectivity, digital systems, and human resources display comparatively stronger overall profiles. A substantial proportion of institutions in these domains are classified as having relative strength or are in the process of development. This indicates that basic connectivity, campus access, core digital platforms, and foundational ICT staffing arrangements are widely present, even if the depth, integration, or resilience varies across institutions.

In contrast, governance and planning, financial sustainability, and data security show weaker and more uneven patterns. These domains show a higher concentration of institutions flagged as priority areas, alongside a significant proportion classified as insufficient data. In the case of governance and planning, this reflects the common situation where partial policy artefacts or planning documents exist, but there is inconsistent or absent evidence of formal approval, operationalisation, or sustained oversight. Financial sustainability also has a divided profile: while a small group of institutions demonstrate relative strength, many lack clear budget lines, diversified funding sources or articulated sustainability mechanisms. In several cases, the available evidence is too limited to permit a confident assessment. Data security and risk management show the most fragmented distribution, combining pockets of relative strength with both priority areas and insufficient data. This is often driven by ad hoc controls rather than integrated institutional practices.

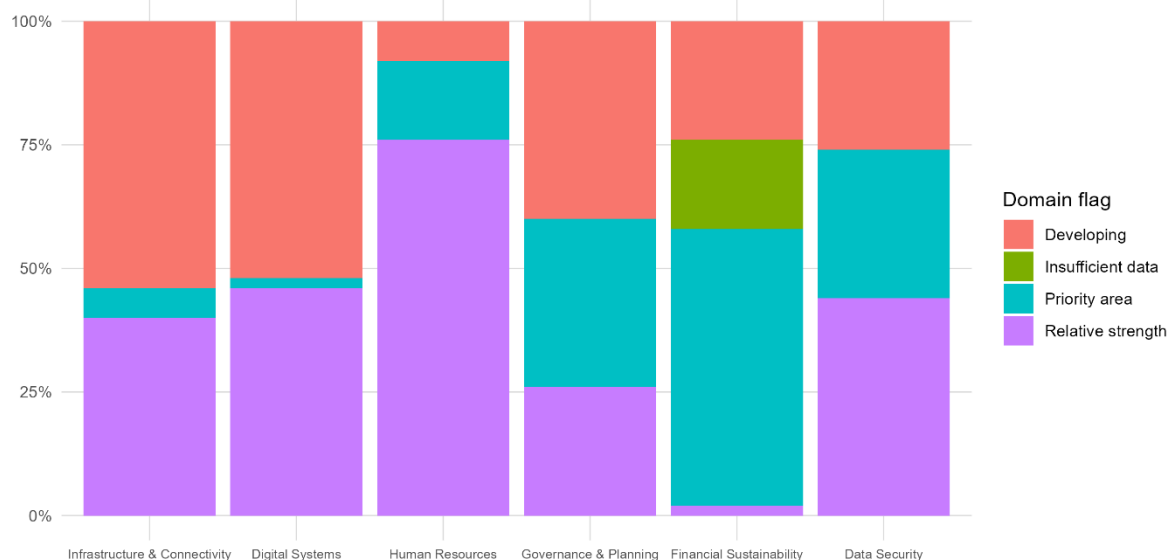


Figure 13: Cross-domain readiness distribution by domain

Figure 14 corroborates these patterns by presenting the average domain score for each institution. The highest average scores are recorded in the infrastructure and connectivity, digital systems, and human resources domains, indicating that basic operational capacity and technical staffing are relatively well

established at a national level. In contrast, governance and planning, as well as financial sustainability, show markedly lower averages, with data security occupying an intermediate position. This supports the idea that governance and financing are systemic constraints rather than isolated institutional weaknesses.

Figure 16 corroborates this by showing the distribution of scores within each domain. While infrastructure, digital systems, and human resources show relatively tight clustering around the mid to upper ranges, governance and planning, and data security exhibit substantial dispersion, with institutions spread across the full score range. Financial sustainability is similarly skewed towards lower and mid-range values. These distributions suggest that national averages conceal significant internal variation, particularly in institutionalised and risk-related domains, where readiness levels are uneven rather than converging around a shared baseline.

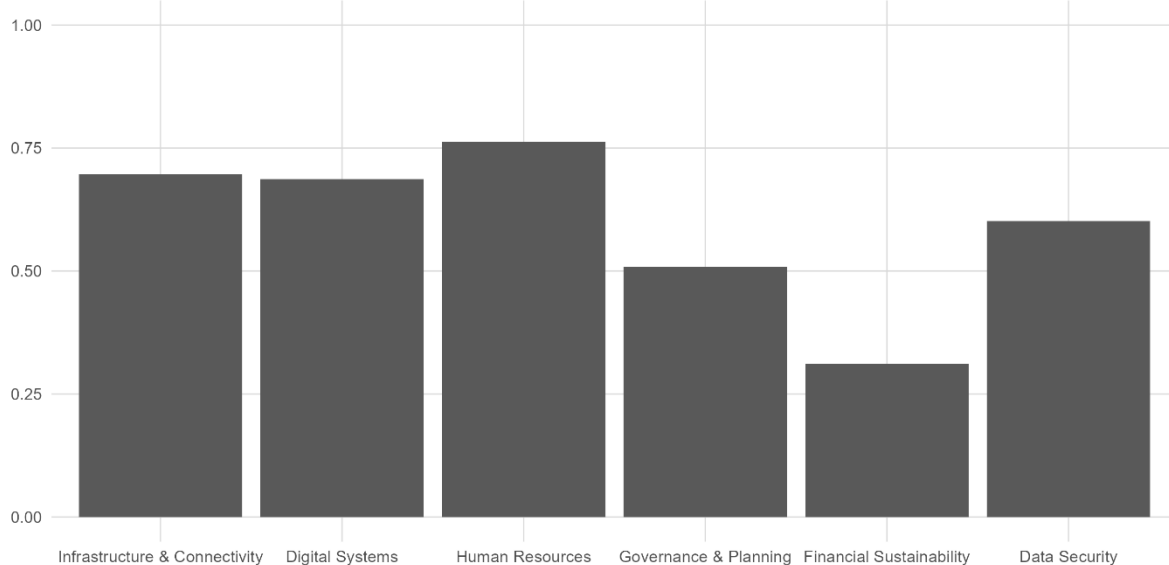


Figure 14: Mean domain scores across institutions

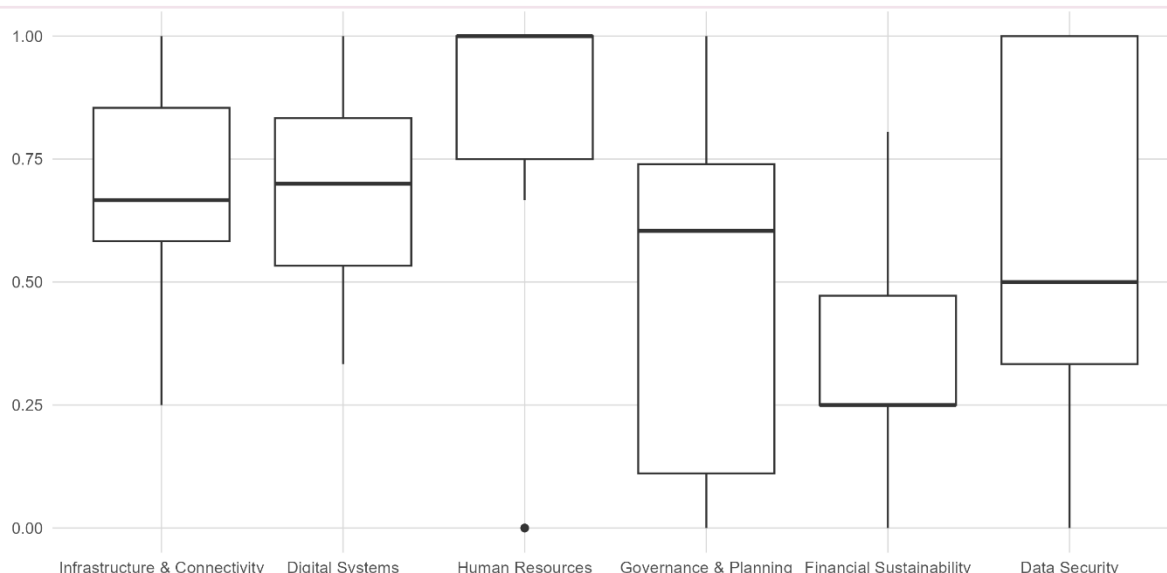


Figure 15: Distribution of scores within each domain

Evidence coverage is an important qualifier of these patterns. As shown in Table 30, coverage is strongest for infrastructure, digital systems and financial indicators, as institutions are better able to report on the existence of assets, systems and budgetary arrangements in these areas. Coverage is more uneven for governance and data security, however,

as these areas rely more heavily on formal documentation and articulated practices, and partial or missing evidence is more common. These gaps in coverage are explicitly accounted for in the scoring and tiering logic and should be interpreted as limitations on confidence rather than implicit judgements of performance.

Table 30: National domain summary

Domain	National readiness pattern (what we observe)	Evidence qualifier (how confident to be and why)
Human resources and ICT organisation	- Strongest-performing domain overall (mean ≈ 0.75–0.78) - A large majority of institutions fall under “Relative strength” (≈ 70–75%), with smaller shares in “Developing” (≈ 15–20%) and “Priority area” (≈ 10–15%) - Suggests that most HEIs report basic ICT organisational structures or roles, even where other domains lag	- Evidence is generally stronger and more complete, as HR indicators are comparatively straightforward to report (existence of ICT units, assigned roles, outsourcing, staff support) - However, “Relative strength” often reflects formal structures on paper, not necessarily depth of capability, workload adequacy, or skills maturity

Infrastructure and connectivity	- Consistently moderate-to-strong but uneven (mean ≈ 0.65–0.70) - The domain is dominated by “Developing” (≈ 55–60%) and “Relative strength” (≈ 35–40%), with very few institutions flagged as “Priority area” ($\approx 5\%$) - Pattern aligns with “connectivity is present, but not consistently robust, resilient, or institution-wide.”	- Evidence coverage is generally high for connectivity and basic infrastructure indicators - Some indicators are susceptible to optimistic interpretation (e.g. reporting connectivity without accounting for reliability, redundancy, or bandwidth adequacy) - Results should be interpreted as availability signals, not performance assurance
Digital systems and learning technologies	- Mid-to-high overall performance (mean ≈ 0.65–0.70) - Institutions are split mainly between “Developing” (≈ 50–55%) and “Relative strength” (≈ 40–45%), with very few flagged as “Priority area” (≈ 0–5%) - Many HEIs report having core administrative or learning systems, but depth of use and integration varies	- Evidence is relatively stable for indicators related to system existence and basic use - Evidence is weaker for pedagogical integration, quality of use, and institutional embedding - Reported adoption should be read as system presence, not necessarily effective or transformative use
Financial sustainability	- Moderately weak and uneven overall (mean ≈ 0.55–0.60) - Most institutions are classified as “Developing” (≈ 50–55%), with a substantial “Priority area” share (≈ 20–25%) and a smaller group demonstrating “Relative strength” (≈ 25–30%) - Indicates fragmented budgeting practices, limited funding diversification, and weak sustainability mechanisms	- This domain is highly sensitive to missing or partial responses (budgets, funding sources, sustainability planning) “Developing” and “Priority area” classifications reflect documented financial governance, not informal coping capacity or ad-hoc funding access - Interpret cautiously where coverage is low or uneven
Data security and protection	- Lower overall performance with high internal variation (mean ≈ 0.55–0.60) - Institutions are spread across “Relative strength” (≈ 40–45%), “Developing” (≈ 25–30%), and “Priority area” (≈ 25–30%) - Signals uneven security maturity, often driven by partial controls rather than integrated risk management	- Evidence coverage is weaker and more inconsistent, particularly for controls-based indicators (incident management, access control, risk assessment) - Where evidence is missing, scores are treated conservatively as “not evidenced” rather than “absent.”
ICT governance and planning	- Weakest domain overall and most polarised (mean ≈ 0.50–0.55) “Developing” (≈ 40–45%) and “Priority area” (≈ 30–35%) dominate, with a smaller share in “Relative strength” (≈ 20–25%) - Represents the clearest national constraint, with limited coherence between strategy, policy, and oversight mechanisms	- Evidence often depends on the availability of formal documents, approvals, and governance structures - This domain is particularly exposed to documentation gaps - Results should be interpreted as an indicator of institutionalisation, not intent or aspiration

Source: Domain scores, domain flags, and coverage indicators derived from the institutional e-readiness assessment dataset. Percentages refer to the share of institutions with usable evidence in each domain and may vary slightly by domain due to coverage differences.

4.1.2 Common cross-domain mismatch patterns

Beyond the performance of individual domains, the national picture is characterised by recurring cross-domain mismatches. This occurs when progress in one area is not consistently matched by complementary institutional capacities elsewhere. These patterns are evident at all levels and form the basis for introducing typologies in Section 5.3.

One common pattern is the presence of basic connectivity alongside weak internal campus networks or management practices. For example, institutions may report external internet access and student labs, but lack structured monitoring, redundancy or internal network governance, which limits the effective use and resilience of these resources.

A second pattern involves the existence of core digital systems without corresponding support practices. Learning management systems or administrative platforms are often present but lack formal service management, data governance and staff capacity support, which reduces their institutional impact.

A third pattern involves policies or plans existing in the absence of systematic implementation. Although governance frameworks may be partially documented, they lack clear enforcement mechanisms, review cycles and alignment with budgeting and operational decision-making.

Data protection and continuity practices also demonstrate an imbalance. While backup mechanisms are frequently in place, broader security controls such as access management, incident response planning and risk assessment are less consistently implemented, resulting in uneven risk exposure.

These recurring mismatches are summarised in Table 31, which links each pattern to the underlying domain signals and outlines why they matter from a sequencing perspective. The intent is not to prescribe solutions, but to highlight structural tensions that help explain why institutions with similar overall scores or tiers may exhibit markedly different readiness configurations.

Table 31: Common cross-domain mismatch patterns observed nationally

Observed cross-domain pattern	Underlying domain signals (typical configuration)	Why this pattern matters	Sequencing implication (analytical, not prescriptive)
Connectivity present, but internal networks and management remain weak	Infrastructure and Connectivity often flagged as <i>Developing</i> or <i>Relative strength</i> , while Governance and Planning and Data Security remain <i>Developing</i> or <i>Priority area</i> .	External connectivity alone does not translate into reliable campus-wide access, performance management, or resilience. Weak internal networks constrain effective use of systems and services.	Highlights the importance of sequencing internal network design, monitoring, and governance alongside connectivity expansion, rather than treating connectivity as a standalone achievement.
Core digital systems exist, but support practices are thin	Digital Systems frequently flagged as <i>Developing</i> or <i>Relative strength</i> , while Human Resources, Governance, or Data Security lag.	Systems without adequate support structures (service management, user support, data governance) tend to underperform or degrade over time.	Suggests that system acquisition often outpaces institutional capacity, and that consolidation phases are critical after initial deployment.
Policies and plans exist, but implementation is uneven	Governance and Planning shows mixed flags (often <i>Developing</i>), while Financial Sustainability or operational domains remain weaker.	Formal documents do not automatically translate into coordinated action, budgeting, or accountability. This creates an appearance of readiness without sustained operational effect.	Indicates a transition point where institutions must move from policy formulation to embedded governance and execution mechanisms.
Backups are in place without broader security controls	Data Security indicators show partial strength (e.g. backups present) alongside <i>Priority area</i> flags for access control, incident response, or risk management.	Isolated controls reduce risk only marginally and may create false confidence if not embedded in a wider security framework.	Emphasises that security maturity is cumulative; foundational controls must be complemented by governance, procedures, and testing.
Operational capacity outpaces financial formalisation	Infrastructure, Digital Systems, or Human Resources flagged as <i>Developing</i> or <i>Relative strength</i> , while Financial Sustainability remains <i>Developing</i> or <i>Priority area</i> .	Short-term operational gains may be difficult to sustain without predictable funding, cost recovery, or lifecycle planning.	Highlights financial sustainability as a gating factor for progression to higher readiness tiers rather than a late-stage “add-on.”
Progress is uneven across domains rather than uniformly low	Institutions display a mix of <i>Relative strength</i> , <i>Developing</i> , and <i>Priority area</i> across domains rather than consistently low scores.	Readiness challenges are rarely uniform; they are shaped by institutional history, investment patterns, and external dependencies.	Reinforces the value of typologies within tiers to explain <i>how</i> readiness is configured, not just <i>how far</i> institutions have progressed.

Source: These patterns are derived from aggregated domain flags and tier distributions and are intended to inform the interpretation of national readiness dynamics. They do not imply institutional deficiency or prescribe specific interventions, the latter of which are addressed in later sections.

4.2 Readiness Tiers as the Primary Synthesis Lens

This section introduces readiness tiers as the primary synthesis mechanism of the report, translating the national snapshot of each domain into an interpretable staging framework at institution level. Figure 14 shows how readiness is distributed within each domain (i.e. where “Relative Strength”, “Developing” and “Priority Area” cluster). Tiers consolidate these signals into a single, comparable view of overall institutional progression, capturing how far institutions have advanced when multiple domains are considered together.

4.2.1 Tier framework and interpretation

Figure 14 shows that there is a clear national pattern in the domain snapshot: operational domains (notably infrastructure/connectivity and human resources) tend to score higher than institutionalisation domains (especially governance/planning and, to a lesser extent, data security and financial sustainability). While tiers preserve this reality, they also allow it to be interpreted at the institutional level by answering the following practical question: **given an institution’s combined domain profile, where does it sit on the overall maturity pathway?**

It is important to note that tiers are not intended as a ranking exercise. They serve as an accessible staging device for:

- » Interpreting overall readiness at a glance
- » Supporting peer learning among broadly comparable institutions
- » They also provide a baseline for repeatable self-assessment over time.

4.2.2 Distribution of institutions across tiers

Figure 16 shows that institutions are concentrated in the mid-tiers, with a relatively small group in the top tier. In this dataset, which comprises 50 responding institutions, the tier distribution is as follows:

- » Tier 1 – Foundational: 17 institutions (34%)
- » Tier 2 – Emerging: 31 institutions (62%)
- » Tier 3 – Developing: 2 institutions (4%)
- » Tier 4 – Established: No institutions

Two implications follow directly from this distribution.

- » The absence of Tier 4 institutions indicates the significant amount of work that remains to be done to achieve consolidated digital readiness. Rather than setting an unrealistic benchmark, the empty top tier indicates persistent gaps in governance, sustainability and risk management, which prevent institutions from translating operational progress into system-wide maturity. The results suggest that no institution has yet achieved the combination of operational capability and institutional coherence necessary for long-term, resilient digital transformation.
- » The national system is best characterised as being in transition, with most institutions clustered in Tier 2 and limited progression beyond this. While the majority of institutions have moved beyond foundational access and basic system adoption, few have reached the level at which digital capabilities are embedded, governed and financed sustainably. This aligns with the domain-level patterns in Figure 13, where “Developing” is the dominant state of operational domains, but governance, financial sustainability, and data security remain widespread constraints on upward movement through the tiers.

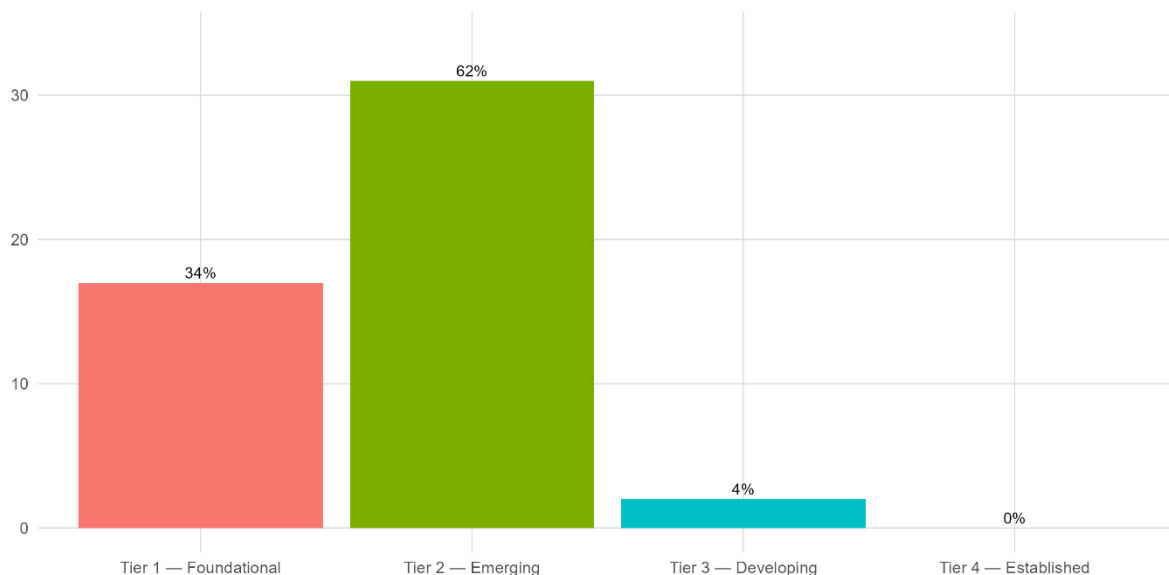


Figure 16: Distribution of institutions by readiness tier

4.2.3 What differentiates tiers nationally

The pattern is not one of uniform, linear improvement. Instead, movement between tiers is determined by whether institutions can translate operational presence (connectivity and systems) into institutional controls (governance, sustainability and security).

» **Tier 1 — Foundational (n = 17; 34%):** Institutions in Tier 1 often demonstrate some operational elements, albeit with limited institutionalisation. On average, overall readiness is low (mean institutional score approximately 0.43), with the strongest signals tending to be in operational areas (e.g. digital systems mean approximately 0.58; infrastructure/connectivity mean approximately 0.58). The absence of formal controls is what most clearly differentiates Tier 1: governance is especially weak (mean ≈ 0.08) and security is inconsistent (mean ≈ 0.48). This profile points to institutions that may be “doing ICT”, but without the structures required to manage it reliably and safely.

» **Tier 2 — Emerging (n = 31; 62%):** Tier 2 represents the primary national readiness category. Institutions in this tier typically have a clearer operational base (digital systems

mean ≈ 0.73 and infrastructure/connectivity mean ≈ 0.75) and materially stronger institutional controls than those in Tier 1, especially in terms of governance (mean ≈ 0.73 compared to 0.08 in Tier 1). However, Tier 2 still reflects incomplete consolidation, with financial sustainability remaining weak (mean ≈ 0.29) and security being uneven (mean ≈ 0.65). In practice, Tier 2 often corresponds to “patchy institutionalisation”: some domains are functional, but readiness is not yet consistently governed, funded and secured.

» **Tier 3 — Developing (n = 2; 4%):** Tier 3 institutions exhibit the strongest cross-domain consolidation in the dataset (mean institutional score ≈ 0.82). They combine strong operational capacity (digital systems mean ≈ 0.90 ; infrastructure/connectivity mean ≈ 0.83) with more consistently present institutional controls (governance mean ≈ 0.79 ; security mean ≈ 0.94) and stronger sustainability signals (financial sustainability mean ≈ 0.58). Given the very small Tier 3 group, these patterns should be treated as indicative rather than definitive, but they still illustrate what “consolidation” looks like in practice.

The tiering results suggest that most institutions have started to develop operational capability, but institutionalisation, especially in terms of governance, security, and sustainable resourcing, is the main constraint on upward movement. This also explains why typologies are useful in the next section: institutions within the same tier can arrive there through different internal configurations, implying different sequencing priorities even when their tier label is the same.

4.3 Typologies Within Tiers

Although readiness tiers summarise overall progress, they can obscure the fact that institutions within the same tier often reach that position through different combinations of strengths and weaknesses. This section therefore introduces typologies within tiers as a secondary analytical tool to explain how readiness is structured across domains among institutions with similar overall scores. These typologies are derived deterministically from the domain flags (“Relative Strength”, “Developing” and “Priority Area”) and are used to support interpretation, sequencing logic and peer learning, without changing tier placement or implying institutional ranking.

4.3.1 Why typologies within tiers

Typologies are nested within tiers and are designed to highlight the most common mismatch patterns within each tier, as discussed in Section 4.1. Rather than introducing a new scoring layer, the typology approach translates each institution’s six-domain flag profile into an interpretable label reflecting the dominant configuration of readiness.

Each typology is defined by a flag “signature” – a small set of recurring combinations that appear frequently in the dataset and have consistent interpretive meaning. For instance, some Tier 2 institutions demonstrate robust operational capabilities (e.g. infrastructure, systems, HR), yet exhibit weaker institutionalisation in areas such as financing and governance. These institutions are categorised under an “operations-led” typology. Conversely, some Tier 1 institutions demonstrate a partial operational presence, yet lack the fundamental institutional infrastructure required to sustain or govern it. This produces a distinct Tier 1 typology. Figure 17 visualises the domain flag signatures that underpin each typology, illustrating how typologies capture recurring configurations of strengths and gaps rather than uniform performance across domains.

Two cautions apply when interpreting typologies. Firstly, typologies are descriptive, not prescriptive; they summarise observed configurations and should not be treated as judgements of performance. Secondly, typologies are only as robust as the underlying evidence. Where documentation is incomplete, particularly in governance and security, typology assignment should be interpreted as “not evidenced” rather than “absent”. For this reason, typologies are best used alongside the domain narrative and evidence qualifiers in Section 4.1 and Table 32.

Table 32: Typology definitions and domain flag signatures

Typology code and label	Short definition (what it represents)	Domain flag signature (typical configuration across domains)
T1-A: Operational Presence, Institutional Void	Institutions with visible operational elements (basic connectivity and digital systems) but weak or missing institutional foundations. Governance, financial sustainability, data security and HR structures are insufficient to support reliability or scale.	- Digital Systems: Developing / Relative strength - Infrastructure and Connectivity: Developing - Governance and Planning: Priority area - Financial Sustainability: Priority area - Data Security: Priority area - Human Resources: Priority area / Developing
T1-B: Infrastructure-Forward, Governance-Constrained	Foundational institutions where connectivity and infrastructure are comparatively strong, but governance and planning form the primary binding constraint, often accompanied by weak sustainability and security practices.	- Infrastructure and Connectivity: Relative strength - Digital Systems: Developing / Relative strength - Governance and Planning: Priority area - Financial Sustainability: Priority area / Developing - Data Security: Developing - Human Resources: Developing
T1-C: Fragmented Readiness	Institutions showing uneven readiness: pockets of capacity coexist with multiple critical gaps. Progress is not uniformly low but lacks coherence across domains.	- Mixed profile with ≥ 2 domains flagged Priority area - Remaining domains split between Developing and occasional Relative strength - Commonly: Governance and Planning and Financial Sustainability as Priority areas
T2-A: Operations-Led with Sustainability Gaps	Emerging institutions with clear operational capability (systems, infrastructure, HR) but persistent weaknesses in financial sustainability and/or governance that limit consolidation.	- Infrastructure and Connectivity: Developing / Relative strength - Digital Systems: Relative strength - Human Resources: Relative strength - Governance and Planning: Developing / Priority area - Financial Sustainability: Priority area (binding gap) - Data Security: Developing
T2-B: Governance-Led, Implementation Catch-Up	Institutions where governance and planning frameworks are relatively advanced, but operational implementation, system depth, or infrastructure reliability lag behind formal intent.	- Governance and Planning: Relative strength - Data Security: Developing / Relative strength - Infrastructure and Connectivity: Developing - Digital Systems: Developing - Financial Sustainability: Priority area / Developing - Human Resources: Developing
T2-C: Uneven Advancement	Institutions making real progress across several domains but lacking coherence. Advancement is visible, yet consolidation is incomplete due to lingering institutional or sustainability constraints.	- Combination of Relative strength and Developing across operational domains - At least one institutional domain (often Financial Sustainability or Governance) flagged Priority area - No consistent cross-domain anchor
T3-A: Broadly Balanced, Selective Gaps	More mature institutions with coherent readiness across most domains, but one or two lagging areas prevent transition to the highest readiness tier.	- Most domains: Relative strength 1–2 domains: Developing (selective gaps) - Priority areas: rare or absent - Typical lag domains: Financial Sustainability and/or Data Security

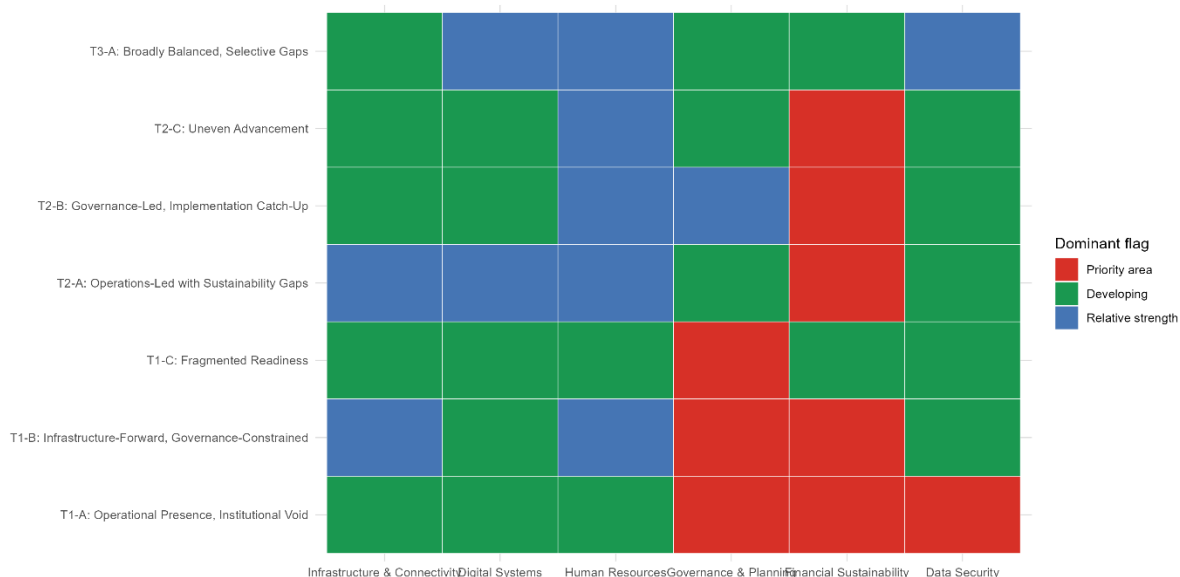


Figure 17: Domain flag signatures underlying readiness typologies

Figure 18 shows the distribution of typologies within each tier, while Figure

19 illustrates the overall prevalence of typologies across the entire sample.

4.3.2 Typology distribution within tiers

Figure 18 summarises the distribution of typologies within each tier of readiness. The results show that variation within tiers is structured rather than incidental, with

a small number of recurring institutional configurations accounting for the majority of institutions at each stage of readiness.

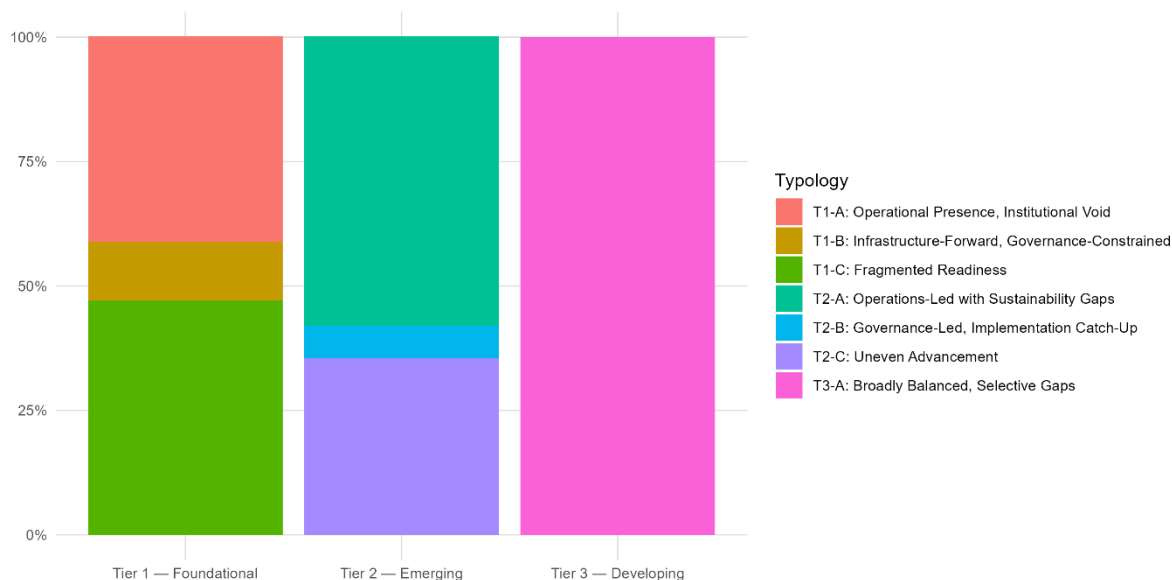


Figure 18: Distribution of typologies within readiness tiers

Within Tier 1, typologies are dominated by Fragmented Readiness (T1-C) and Operational Presence, Institutional Void (T1-A). This suggests that foundational institutions rarely encounter a single binding constraint, but rather exhibit overlapping weaknesses in governance,

sustainability and security, even where basic infrastructure or systems are in place.

In Tier 2, typological diversity increases, but remains patterned. Most institutions follow an operations-led trajectory

with sustainability gaps (T2-A), while a substantial minority exhibit uneven advancement across domains (T2-C). A small number of institutions display governance-led profiles with implementation catch-up needs (T2-B). Together, these patterns suggest that Tier 2 represents a consolidation phase, during which time institutions struggle to align operational growth with formal controls and long-term viability.

Tier 3 institutions are uniformly classified as Broadly Balanced with Selective Gaps (T3-A). While these institutions demonstrate stronger cross-domain coherence than those in lower tiers, they

still exhibit specific weaknesses that prevent them from reaching full maturity. This reinforces the idea that Tier 3 is a stage of partial, rather than complete, institutional consolidation.

Figure 19 illustrates this trend at a national level, revealing that a small number of typologies, particularly “Fragmented Readiness” (T1-C) and “Operations-Led with Sustainability Gaps” (T2-A), account for a significant proportion of institutions. This concentration indicates that digital readiness challenges are not randomly distributed, but rather cluster around a limited set of recurring institutional trajectories.

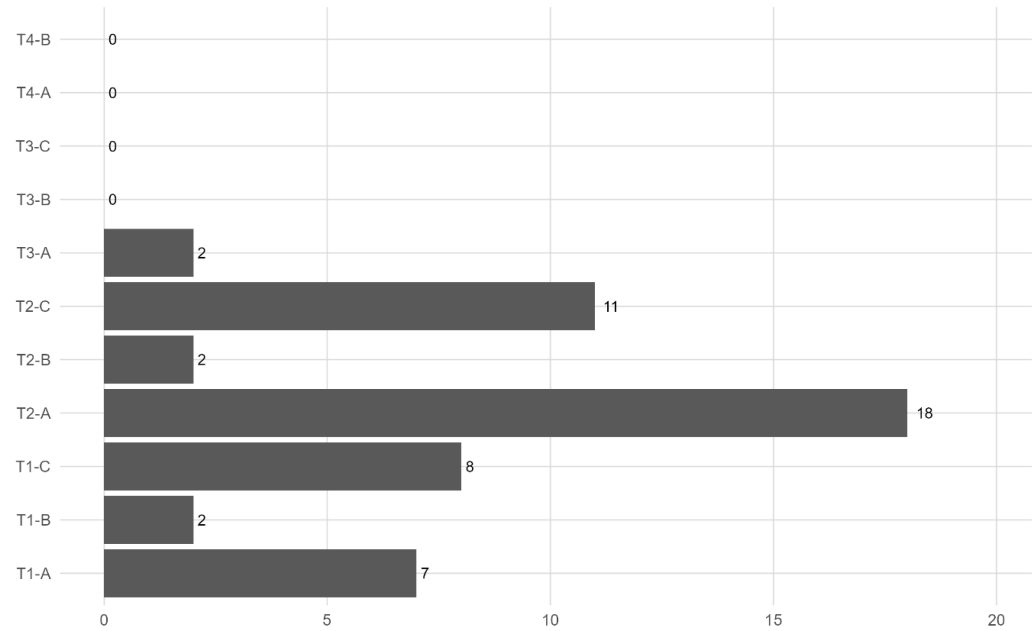


Figure 19: Overall prevalence of readiness typologies across institutions

4.3.3 Typologies by tier

This subsection presents typologies tier by tier, emphasising that they are nested within readiness tiers and used to explain variation within tiers, rather than creating an alternative hierarchy.

The discussion highlights how institutions at similar overall levels of readiness can still exhibit different combinations of strengths and limitations, which has implications for sequencing and interpretation.

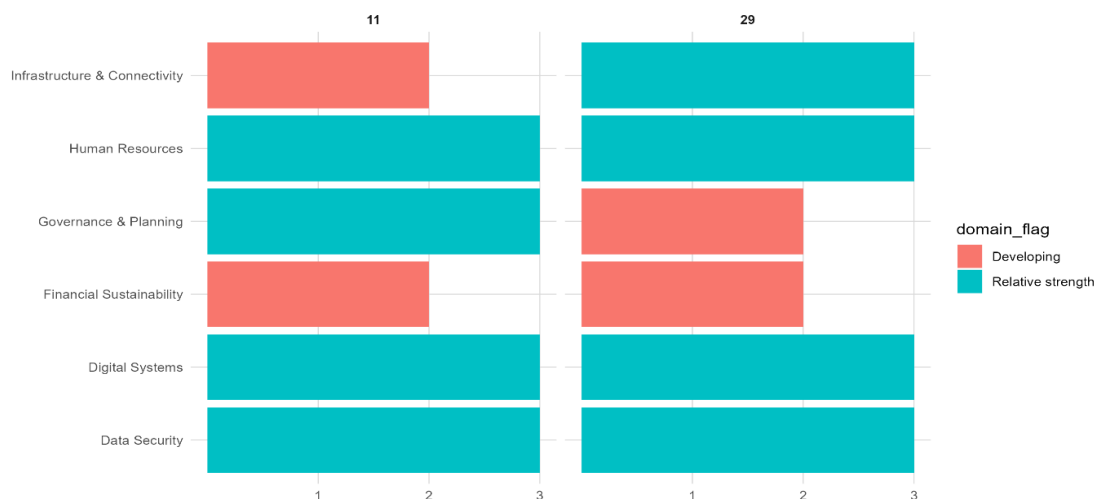


Figure 20: Domain flag profiles of tier 3 institutions

Figure 20 shows that even among Tier 3 institutions, which are considered to be at the highest level of readiness in this assessment, residual operational and institutional constraints remain evident. This supports the view that Tier 3 represents an advanced but incomplete stage of consolidation rather than full maturity.

Tier 1 – Foundational: Multiple constraints, uneven baselines

Tier 1 institutions are characterised by the absence of a consolidated institutional baseline. This is reflected in the dominance of typologies that signal fragmentation and structural gaps, rather than isolated weaknesses. As shown in Table 32, T1-C: Fragmented Readiness accounts for the largest proportion of Tier 1 institutions. These institutions display mixed domain signals, with pockets of relative strength coexisting alongside multiple priority areas, most commonly in governance and planning, data security, and financial sustainability. This indicates that readiness challenges at this level are rarely confined to a single domain or linear.

Two smaller typologies capture more specific Tier 1 configurations. T1-B: Infrastructure-Forward, Governance-Constrained reflects institutions where basic connectivity and systems are in place, but weak governance and planning constitute binding constraints. T1-A, “Operational Presence, Institutional Void”, represents a sharper imbalance, where limited operational capability

exists in the near absence of institutional scaffolding. Together, the Tier 1 typologies suggest a fundamental challenge of institutionalisation rather than a mere lack of infrastructure or technology.

Tier 2 – Emerging: Divergent consolidation pathways

Tier 2 institutions fall into two main categories, showing that “emergence” does not follow a single trajectory. T2-A, “Operations-Led with Sustainability Gaps”, captures institutions that have made visible progress in operational domains, such as infrastructure, systems and human resources, but where financial sustainability and governance lag behind. In these cases, the limiting factor is no longer access or adoption, but the formalisation and stabilisation required to maintain progress.

By contrast, T2-C: Uneven Advancement, reflects institutions where progress is inconsistent across domains, with at least one underdeveloped area alongside one or more relatively strong domains. This typology indicates the need for consolidation across multiple fronts rather than targeted correction in a single area. The coexistence of these typologies within Tier 2 suggests that, despite being at similar overall readiness levels, institutions may face qualitatively different next-stage challenges.

Tier 3 – Developing: Institutional form outpacing execution.

Tier 3 represents the highest level of readiness observed in the dataset. While institutions at this level exhibit broadly coherent cross-domain performance, Figure 5.8 shows that selective gaps persist even at this stage. These gaps are most commonly operational rather than structural, suggesting that the main challenge has shifted from establishing the institution to executing its activities effectively.

All Tier 3 institutions fall under T3-A: Broadly Balanced, Selective Gaps. This typology is characterised by relative strength across most domains, alongside one or two areas of weakness, which are often related to financial sustainability or governance implementation. This suggests that Tier 3 institutions are no longer constrained by fragmented readiness, but rather by the difficulty of fully embedding and operationalising institutional frameworks.

The absence of additional Tier 3 typologies reflects the small number of institutions at this level and the conservative tiering logic applied. It is important to note that the Tier 3 profile should not be interpreted as “fully mature”, but rather as an advanced transitional stage in which targeted interventions can yield disproportionate gains.

Overall implication

The nested typology analysis confirms that the readiness tiers reflect the progress made by institutions, while the typologies illustrate how readiness is implemented in practice. Movement between tiers is restricted by institutional thresholds, whereas variation within tiers reflects different combinations of structural and institutional bottlenecks. This distinction is crucial for implementation planning, as discussed further in Section 4.4.

4.4 Structural vs Institutional Bottlenecks

This section distinguishes between structural bottlenecks, which lie largely outside the control of individual institutions, and institutional bottlenecks, arising from internal governance, organisational and management practices. Structural bottlenecks shape what institutions can realistically achieve, while institutional bottlenecks determine how effectively available resources are governed and sustained. This distinction is important when interpreting readiness tiers and typologies, since institutions at similar tiers may be affected by different fundamental factors. This has implications for how readiness gaps should be understood at a system level.

4.4.1 Structural bottlenecks: System-level constraints shaping readiness

Structural bottlenecks are most evident in areas where performance is influenced by sector-wide conditions, shared infrastructure, or national policies and financial environments, rather than by the choices of individual institutions alone. In the Somali higher education context, these bottlenecks are most evident in terms of infrastructure and connectivity, financial sustainability, and key aspects of data security.

Many institutions across tiers report having basic connectivity and core digital systems in place, yet they remain constrained by external factors such as unreliable power supplies, limited upstream bandwidth, dependence on commercial internet service providers and the absence of shared services or sector-level platforms. These conditions help to explain why infrastructure and connectivity frequently appear as “developing” even among Tier 3 institutions, and why even the most advanced institutions still exhibit selective operational gaps rather than fully consolidated performance. The persistence of these constraints is reflected in typologies characterised by balanced readiness with residual weaknesses rather than uniform strength across domains.

Financial sustainability also exhibits strong structural characteristics. Although budgeting practices and internal cost controls are the responsibility of institutions, the extent to which they can formalise these practices is heavily influenced by the availability of predictable funding streams, donor coordination, and sector-level financing mechanisms. This dynamic is particularly evident in T2-A: Operations-Led with Sustainability Gaps, where progress in infrastructure, systems and staffing has outpaced the development of stable financing arrangements. In such cases, the bottleneck reflects institutional sequencing choices as well as an uncertain and fragmented funding environment that limits long-term planning and consolidation.

Finally, data security and risk management display a hybrid structural character. Institutions often depend on external service providers, shared hosting environments or informal arrangements, which restricts their ability to implement comprehensive controls independently. Consequently, partial measures, such as basic backups or ad hoc access controls, may be implemented without the broader institutional, technical or contractual foundations required for systematic risk management. This pattern contributes to data security remaining a priority or developing domain across multiple tiers, even where other aspects of readiness are more advanced.

4.4.2 Institutional bottlenecks: Internal capacity and coherence gaps

Institutional bottlenecks arise from the way in which institutions organise, govern and implement their digital functions. Unlike structural constraints, these bottlenecks are primarily internal, manifesting most clearly in governance, planning, and human resources. They are strongly associated with tier progression, particularly when moving beyond the foundational and early emerging stages.

Governance and planning emerge as consistent constraints across all tiers, but are most pronounced in the Tier

1 and Tier 2 typologies, including T1-C: Fragmented Readiness and T2-C: Uneven Advancement. In these configurations, the issue is not a lack of intent or isolated initiatives, but rather a lack of coherent institutional links between strategy, policy, budgeting and operational decision-making. Fragmented documentation, unclear mandates and weak oversight mechanisms limit the ability of institutions to prioritise investments, coordinate actions across units or sustain progress over time. Consequently, existing assets and capabilities are frequently underutilised or deployed opportunistically rather than strategically.

Human resources present a related but distinct institutional bottleneck. While many institutions report having ICT staff or dedicated units, typologies such as T3-A: Broadly Balanced and T2-A: Operations-Led with Sustainability Gaps indicate that role clarity, workload balance and professional development often fall behind operational demands. In these cases, although staffing exists, institutional arrangements do not adequately support effective execution, leading to bottlenecks in system maintenance, user support, and policy implementation.

Across multiple typologies, institutional bottlenecks are therefore best understood as problems of misalignment rather than absence. Systems, policies or staff may be present, but weak coordination between them limits impact. This explains why institutions with similar domain scores or tier placements can experience markedly different operational realities.

4.4.3 How can tiers and typologies be used to distinguish between different types of bottleneck?

Together, readiness tiers and typologies provide a structured way to identify the dominant bottleneck and the most effective type of intervention. Tiers indicate how far institutions have progressed overall, while typologies reveal why progress has stalled or become uneven at a given stage.

Lower tiers tend to reflect compounded institutional bottlenecks, where multiple foundational elements — such as governance, staffing, and basic coordination mechanisms — are weak or absent simultaneously. As institutions progress to Tier 2 and Tier 3, the nature of the bottleneck usually shifts from basic access or adoption to issues of coherence, execution and sustainability. At these levels, the challenge becomes less about introducing new systems and more about ensuring that existing systems work together reliably and at scale.

Typologies refine this analysis by distinguishing between structural constraints, such as residual infrastructure or financing issues that persist despite internal efforts, and institutional constraints, such as governance, planning or sustainability issues that limit performance even when resources and systems are available. This distinction is analytically important. Structural bottlenecks can obscure strong institutional effort and progress, while institutional bottlenecks can suppress outcomes despite comparatively favourable operating conditions.

4.4.4 Implications for national interpretation

At the national level, the distribution of typologies suggests that many readiness constraints in Somali higher education are not purely technological. Instead, they arise from the interaction between a challenging operating environment and uneven institutionalisation within institutions. Therefore, recognising whether a bottleneck is structural or institutional is essential for fairly interpreting readiness results and for sequencing future interventions. These implications are explored further in Chapter 8, which translates the analytical distinctions established here into policy and investment considerations.

5 Regional Benchmarking: Somalia in Comparative Perspective

Chapter 6 provides a comparative analysis of Somalia's higher education e-readiness results, using regional reference points to interpret readiness patterns rather than ranking performance. Building on the national synthesis in Chapter 5, the benchmarking focuses on how readiness is configured across domains: where capabilities are widespread, where they are uneven and where cross-domain mismatches suggest bottlenecks that could hinder progression despite the presence of operational foundations. The aim is to refine the interpretation of Somalia's readiness "shape" and typical bottleneck profiles while explicitly acknowledging comparability limitations and avoiding causal claims.

5.1 Purpose and Scope

This benchmarking exercise is designed to be directional and illustrative. It provides a structured way to interpret Somalia's national readiness pattern (as established in Chapter 5) alongside selected regional comparators. This clarifies what is systemically constrained, what is institutionally uneven and where Somalia shows relative strengths or gaps by domain. The intent is explanatory: to contextualise the SomaliREN institutional baseline, not to score countries or certify performance.

Benchmarking is limited to institutional readiness patterns across the six domains used in this assessment: Infrastructure and Connectivity, Digital Systems, Human Resources, Governance and Planning, Financial Sustainability and Data Security. The unit of analysis is the higher education institution, and the findings are interpreted at an aggregated national level and through groupings such as tiers and typologies (without identifying institutions). Comparisons are used to understand how Somalia's domain configuration and mismatch patterns relate to trajectories observed in systems with more mature higher education connectivity and coordination arrangements.

Kenya, Uganda and Rwanda are used as illustrative reference points. They were selected because they represent different regional pathways of higher education, digital development, and NREN ecosystem maturity. They also offer sufficient publicly documented evidence to support careful, domain-level comparisons. The comparator countries are not treated as targets or gold standards; they are used to expand the scope of interpretation and reduce the risk of interpreting Somalia's results in isolation.

Cross-country differences are primarily treated as reflections of structural and system-level conditions, such as national backbone depth, NREN mandate and reach, coordination capacity, shared service maturity and funding models, rather than as proxies for institutional effort. Where Somalia appears "behind", "comparable", or "ahead in pockets", the interpretation links back to the logic in Chapter 5: higher tiers tend to shift bottlenecks from access/adoption towards coherence, execution capacity, sustainability, and security, and typologies help to distinguish which bottleneck dominates within similar overall readiness levels.

Benchmarking is constrained by uneven data availability across countries and domains, differences in the years of the studies, and differences in what is measured and reported. The chapter therefore prioritises transparency and conservatism: it compares domain patterns and enabling conditions, and it notes gaps where evidence is lacking rather than filling them with inferences.

5.2 Benchmarking Framework and Method

Benchmarking is used to compare the e-readiness of Somalia's higher education system against that of peer countries (Kenya, Rwanda and Uganda) across six domains: Infrastructure and Connectivity, Digital Systems, Human Resources, Governance and Planning, Financial Sustainability and Data Security. These domains are divided into four readiness bands: **Foundational, Emerging, Developing and Established**. No numeric scores or rankings are used. Instead, each country's position in a domain is determined by triangulating multiple indicators based on available national and institutional-level evidence.

The sources and evidence base draw from three main categories:

» **NREN documentation:** For example, Kenya Education Network (KENET), Kenya's NREN (with 231 member institutions as of 2025)¹⁰ provides robust data on connectivity, service uptake and backbone reach. The Research and Education Network for Uganda (RENU) reports over 1000 connected sites as of 2025 and has a long-term expansion strategy that includes lower education levels.¹¹ Rwanda Education Network (RwEdNet), which is now embedded within the Ministry of Education, surpassed 1,000 connected education sites by 2023 and had a target of 1,500 by mid-2024.¹²

» **Higher education sector studies:** The 2022 KENET Core Data Survey includes LMS deployment (49 out of 54 universities), the presence of a disaster recovery site (only 11 universities) and general ICT infrastructure trends. In Uganda, World Bank assessments and RENU evaluations provide campus-level connectivity and staffing indicators.

Data on Rwanda's digital systems is limited, with proxy indicators derived from national education and ICT strategies.

» **Policy frameworks:** Kenya, Rwanda and Uganda have data protection laws that require local data storage or equivalent jurisdictional safeguards, influencing university compliance behaviour.^{13,14} All three have active cybersecurity strategies and national ICT plans that guide institutional digital practices.

The level of e-readiness is assessed for each domain using a four-tier readiness band rubric, which provides a qualitative description:

- » **Foundational:** minimal or ad hoc development (e.g. basic ISP connectivity with no NREN integration)
- » **Emerging:** partial uptake or policy presence (e.g. some institutions have an LMS or ICT plan, but staffing is patchy).
- » **Developing:** widespread implementation, but with gaps in quality and coverage (e.g. most institutions are connected, but there is uneven bandwidth or HR capacity).
- » **Established:** sector-wide maturity and institutionalisation (e.g. recurring ICT budgets, disaster recovery sites and data compliance frameworks).

Indicators used for band placement include NREN coverage, campus bandwidth, LMS adoption, ICT staffing ratios, institutional ICT plans, funding mechanisms, backup and disaster recovery measures, and compliance with data protection policies.

10 KENET membership <https://www.kenet.or.ke/content/list-kenet-members>

11 RENU services <https://renu.ac.ug/services/>

12 RwEdNet <https://africaconnect3.net/rwednet-roars-back-to-life/>

13 <https://www.risa.gov.rw/data-protection-and-privacy-law>

14 https://pdpo.go.ug/media//2022/03/Data_Protection_and_Privacy_Act_No_9_of_2019.pdf

As this qualitative benchmarking draws on varied data, it is accompanied by careful notes on limitations of comparability. These include:

- » The country's unique context is taken into account, such as system size, resources, investment levels and historical constraints
- » Evidence varies by year
- » Institutional coverage and definitions differ across countries, so comparisons prioritise university-level data
- » Legal obligations (e.g. Kenya's enforced DPA vs. the absence of an equivalent law in Somalia) influence the meaning of "compliance" in each country
- » Where data is missing or non-specific (e.g. LMS usage in Rwanda), this is noted and not inferred.

This framework underpins the country-by-country domain analysis in Section 6.3, enabling descriptors such as "behind but improving" or "comparable in pockets" to be linked to real readiness conditions rather than broad reputational assumptions. Each band assignment reflects a consolidated judgement based on the available evidence, rather than calculated thresholds.

5.3 Comparative National Readiness by Domain

This section provides a comparative analysis of Somalia's higher education e-readiness by reviewing each of the six domains against reference points from Kenya, Uganda and Rwanda. The objective is to conduct directional benchmarking, interpreting Somalia's readiness configuration rather than ranking countries, by identifying areas where institutional capacity is relatively well-established (e.g. connectivity and core systems) versus areas where institutionalisation and risk management are less embedded (e.g. financing discipline, governance coherence and security practices). Each subsection has a consistent structure comprising a brief Somalia overview drawn from Chapter 5, reference points from the comparator countries, the placement of the qualitative readiness bands, and a brief explanation of the structural drivers that could account for the observed differences. To provide a consistent narrative across the domains and support coherence between the subsections, Table 33 summarises the national readiness positioning by domain for all four countries and serves as the core "at-a-glance" benchmark for the subsection.

Table 33: National readiness positioning by domain

Domain	Somalia	Kenya	Uganda	Rwanda
ICT Infrastructure and Systems	Emerging	Established	Established	Developing
Human Resources and Capacity	Foundational	Developing	Developing	Emerging
ICT Governance and Strategy	Emerging	Developing	Developing	Developing
Core Digital Systems	Foundational	Developing	Emerging/ Developing	Developing
ICT Budgeting and Allocation	Foundational	Developing	Emerging/ Developing	Developing
System and Network Security	Foundational	Developing	Developing	Developing

5.3.1 Infrastructure and connectivity

Higher education connectivity in Somalia has shown meaningful progress alongside significant variation in coverage and service quality. Institutions connected via SomaliREN typically perform better than those that rely on ad hoc commercial links. Even where upstream connectivity exists, constraints around bandwidth, scale, reliability and limited redundancy continue to affect the user experience and the ability to deliver consistent campus connectivity on a daily basis.^{15,16,17} The detailed Somali baseline is set out in Chapter 5 and is used here as the domestic reference point for a regional comparison.

Regional reference points (Kenya, Rwanda and Uganda)

The regional reference points emphasise NREN reach and campus delivery capacity because these signals are the most consistently documented across the peer systems:

Kenya. Kenya's higher education connectivity is supported by a mature NREN (KENET) with wide sector coverage and a service model that combines backbone connectivity with shared services. KENET reports over 200 member institutions (both public and private

institutions) and, by late 2023, had a fibre footprint of 495 connected campuses across 46 counties, indicating near-national reach. Available capacity has increased substantially over time (from ~15 Mbps per 1,000 users in 2016 to ~40 Mbps per 1,000 users by 2021), with many campuses meeting KENET's "high-speed" benchmark (≥ 1 Gbps). Major universities have received multi-gigabit links alongside eduroam and campus digital infrastructure initiatives to improve Wi-Fi and LAN quality.^{18,19} However, evidence also notes periodic fiscal constraints, including bandwidth rationing and a documented dip in 2020.²⁰

Uganda. RENU has expanded rapidly in terms of both its reach and subscribed capacity. It now connects all public universities (10/10) and a majority of private universities, as well as hundreds of other educational and research sites. RENU's footprint grew from 139 member institutions and 216 connected campuses in 2020 to 838 connected sites by the end of 2024. Total subscribed bandwidth rose to ~15 Gbps in 2023 and 18.8 Gbps in 2024. Major campuses operate at a multi-gigabit scale (e.g. Makerere at ~2.0 Gbps), and eduroam is available across dozens of sites. Network development has leveraged national fibre assets and metropolitan rings, with investments in resilience (e.g. redundant routes) and a national data centre to localise traffic.^{21,22,23,24}

15 Keeping students connected in Somalia, <https://blogs.worldbank.org/en/digital-development/keeping-students-connected-somalia>

16 Improved internet access connects Somali students to each other and to global knowledge

<https://blogs.worldbank.org/en/digital-development/improved-internet-access-connects-somali-students-each-other-and-global-knowledge>

17 SomaliREN driving transformation through research and education networking innovation – UbuntuNet Alliance, <https://ubuntunet.net/stories/somaliren-driving-transformation-through-research-and-education-networking-innovation/>

18 KENET website, <https://www.kenet.or.ke/>

19 KENET Impact Report 2023, https://www.kenet.or.ke/sites/default/files/kenet_impact_report_2023_0.pdf

20 https://www.kenet.or.ke/sites/default/files/2021_annual_core_data_report_highlights.pdf

21 RENU services, <https://renu.ac.ug/services/>

22 RENU presentation, https://uvcf.ac.ug/wp-content/uploads/2025/02/RENU-Infrastructure_compressed.pdf

23 <https://kcl.co.ug/wp-content/uploads/2023/01/Circulation-Version-Breaking-the-Final-Connectivity-Barriers-for-Higher-Education-Institutions-in-Africa.pdf>

24 World Bank Group, Feasibility Study to Connect all African Higher Education

Rwanda. Following an earlier NREN setback in 2018, Rwanda's education connectivity has accelerated under a government-led reboot of RwEdNet, implemented under the Smart Education programme and anchored within the Ministry of Education. By July 2024, RwEdNet had connected over 1,000 education sites, which included universities and other tertiary institutions. This was complemented by on-site enablement, including Wi-Fi access points, labs, and end-user devices, as well as an upstream link of 10 Gbps to the UbuntuNet backbone, with plans to scale up to 20 Gbps. As the rebooted NREN is new, institutional policies, technical teams and campus IT infrastructure are still being consolidated, meaning some sites may initially rely on basic access modalities (including LTE where fibre is pending).¹²

Comparative positioning

Readiness bands are qualitative descriptors based on converging signals about coverage, capacity, resilience and institutionalisation. Placements should be read as directional: “Established” reflects sustained, sector-wide capability; “Developing” reflects widespread deployment that is still consolidating; and “Emerging” reflects partial coverage and early institutionalisation.

Kenya is Established: This is due to KENET's maturity, its near-national institutional coverage (including public and private providers), its high-capacity links (often ≥1 Gbps) and its institutionalised shared services supporting resilient academic connectivity.^{18,19,20,24}

Uganda is Established: This is due to RENU's extensive university coverage, substantial connected-site footprint, increasing subscribed bandwidth (tens of Gbps aggregate), eduroam implementation, and investments in resilience, including local hosting and redundant routing.^{21, 23, 24, 24}

Rwanda is Developing: Rwanda is developing because, although connectivity has scaled towards nationwide tertiary coverage (1,000+ sites, expanding towards 1,500), thanks to an extensive national infrastructure, the rebooted NREN is still in the early stages of its operational lifecycle and institutional practices are still being finalised.¹²

Somalia is Emerging: SomaliREN has connected around 20–28 universities (roughly 50–60 campuses), is recognised as a “connected NREN”, and has completed one of three planned backbone segments. However, coverage is not yet comprehensive and bandwidth remains modest in many cases.^{15,16,17,25}

Key explanatory factors

NREN maturity and mandate are central drivers. Kenya and Uganda benefit from long-running networks, while Rwanda's rebooted RwEdNet and Somalia's SomaliREN are still in the consolidation phase.^{12,17,24}

Backbone availability and geography influence the feasibility and cost of expansion. Rwanda's national fibre and last-mile investments have enabled a rapid rollout, whereas Somalia's backbone gaps have constrained expansion beyond key corridors. Market and cost conditions influence scaling: Kenya's competitive ecosystem and IXP development are associated with high local traffic exchange (approximately 70%) and cost efficiencies. In contrast, Somalia faces higher bandwidth prices.^{12,17,24}

Policy support and partnerships affect sustainability. Rwanda has embedded RwEdNet within the government. Kenya and Uganda operate mature, multi-stakeholder NREN ecosystems. Somalia's early growth has relied heavily on donor-supported programmes.^{12,17}

Institutions to High-Speed Internet (Vol. 1 of 3) <http://documents.worldbank.org/curated/en/320071626434508906>

25 SomaliREN succeeds in implementing the international service of eduroam | AfricaConnect3 <https://africconnect3.net/somaliren-succeeds-in-implementing-the-international-service-of-eduroam/>

5.3.2 Digital systems

Somalia's digital systems for higher education remain in their infancy. Many universities rely on ad hoc or basic digital platforms at best. For instance, while a few institutions have set up an LMS, these are used minimally, often merely to upload PDF lecture notes rather than deliver interactive e-learning. Core academic and administrative processes, such as student records, grading and admissions, are still largely handled through manual processes. This means that any digital systems that do exist operate in isolation. While some universities provide institutional email addresses to staff and students, adoption is uneven and many continue to use personal email addresses.

Kenya. Kenyan universities have widely adopted digital systems, particularly LMSs for learning. By 2020, almost all universities had adopted an LMS (mostly Moodle), and the shift to online learning prompted by the pandemic further increased usage. However, the depth of use remains uneven: many lecturers still mainly upload notes to the LMS rather than making use of the interactive features. Major universities run student information systems and online portals, though full interoperability between learning and administrative platforms is not yet commonplace. KENET supports these initiatives by offering shared services such as video conferencing, Eduroam and an academic identity federation (Rafiki). Core systems are in place across the sector, but integration and faculty uptake are still ongoing.^{26,27,28}

26 <https://thekenyatimes.com/latest-kenya-times-news/moi-university-ranked-third-in-offering-blended-degree-programs/>

27 <https://files.eric.ed.gov/fulltext/EJ1102715.pdf>

28 <https://ubuntunet.net/members/the-journey-of-the-first-kenyan-identity-federation-rafiki/>

29 <https://africaconnect3.net/remote-teaching-transforms-learning-at-st-pauls-university/>

30 https://education.asu.edu/sites/g/files/litvpz656/files/2023-12/12-22-2024_J2_Embracing_e-Learning_PWFormatted.pdf

31 <https://ubuntunet.net/stories/renu-identity-federation-rif-joins-edugain/>

32 <https://connect.geant.org/2022/08/16/renu-makes-connectivity-accessible-to-all-through-metro-eduroam>

33 <https://ur.ac.rw/?UR-online-learning-at-a-glance-what-you-need-to-know-about-the-platform>

34 <https://epaa.asu.edu/index.php/epaa/article/download/8772/3538/42257>

35 <https://ur.ac.rw/?UR-gets-smart-classroom-to-facilitate-e-learning>

Uganda. Before the pandemic, very few institutions offered online programmes (less than 10%) and campus LMSs were rarely used. Post-pandemic, however, most have adopted or upgraded their LMS and begun incorporating online content into their teaching, despite ongoing content and access challenges. RENU has played a pivotal role in this, providing an academic identity federation (an eduGAIN member since 2018), extensive eduroam Wi-Fi (with over 500 hotspots by 2024), and cloud services for e-learning and backups. This has enabled smaller institutions to establish an online presence. Nevertheless, usage and integration remain inconsistent – many systems operate in isolation and some faculty members and students are reluctant to adapt.^{27,29,30,31,32}

Rwanda. In 2020, a government mandate pushed all higher education institutions (HEIs) to implement e-learning, with the University of Rwanda (UR) moving nearly all courses online during the lockdown caused by the pandemic. Measures such as zero-rated educational internet helped other colleges follow suit, though adoption outside UR was inconsistent. The UR has also set up a “smart classroom” and is developing an integrated information system to replace manual records. However, most Rwandan HEIs still lack advanced MIS/ERP platforms. RwEdNet remains limited, but an identity federation is under discussion and Rwanda has not yet joined eduGAIN.^{33,34,35}

Comparative positioning

Kenya is Developing. Core e-learning and admin systems are widely available with the support of KENET, but integration and uptake by faculty remain uneven.

Uganda is Developing. While most institutions adopted LMS and RENU-facilitated tools after 2020, usage and interoperability remain inconsistent. NREN support has driven broad adoption, but the depth of use and interoperability remain uneven overall.

Rwanda is Emerging. While the UR and a few others are approaching a developing-level digital capacity, many institutions are still in the basic pilot stage. Key platforms exist and are demonstrated at UR, but digital use and integration across the sector is still in its infancy and fragmented overall.

Somalia is Foundational. Digital systems are largely absent and most university operations remain manual and offline.

Key explanatory factors

NREN-enabled services in Kenya and Uganda. KENET and RENU provide sector-wide digital services, such as a national e-learning platform, eduroam Wi-Fi across campuses and academic identity federation. These services have significantly enhanced the digital capacity of universities. During and after the pandemic, the NRENs supported most universities in rolling out LMS and online classes with the help of the regulator, though skill gaps and access issues persisted.^{11,26,29,30}

Rwanda's policy-driven leap. In 2020, the Rwandan government mandated e-learning, and the country's flagship university, UR, uploaded 91% of its courses to a Moodle platform within weeks. Other institutions attempted to follow suit with the support of zero-rated internet, but many struggled due to a lack of content and infrastructure. This top-down approach explains Rwanda's emerging status: UR achieved near-full LMS usage, yet most smaller universities remain at an early stage of adoption.^{33,34,35}

NREN maturity as a driver. Kenya and Uganda's advanced NRENs (KENET and

RENU) offer affordable bandwidth, cloud hosting, eduroam and single sign-on, enabling even smaller campuses to adopt digital systems. By contrast, the minimal reach of SomaliREN and the ongoing development of RwEdNet in Rwanda mean that institutions in these countries lack shared services and must rely on their own limited resources.

Policy and coordination differences. Rwanda's strict e-learning mandate and "Smart Classroom" initiative meant that all universities tried online learning in 2020. Meanwhile, Kenya's policies (via CUE and partnerships with telecoms companies) fostered an environment conducive to e-learning. Uganda had no comprehensive policy prior to the pandemic and only moved when forced by circumstances, while Somalia has no national digital education policy at all. This explains why adoption in Somalia has been ad hoc and slower.³⁰

Impact of institutional diversity. Kenya's large and diverse higher education sector includes well-resourced universities that are pioneering digital adoption, as well as smaller institutions that are lagging behind. This necessitates strong coordination to avoid "islands of automation". Meanwhile, Rwanda's sector is dominated by the University of Rwanda (UR) – its rapid progress has lifted national averages but has also highlighted that other colleges lack a similar capacity. This diversity affects how uniformly digital readiness improvements are spread within each country.

5.3.3 Human resources

In the Somali sample, the Human Resources and ICT organisation domain is the strongest (mean ≈ 0.77), with $\sim 77\%$ of institutions flagged as having "relative strength", indicating that many HEIs report basic ICT structures and roles. This signal is based on simple self-reports and often reflects "structure on paper", rather than depth of capability. Evidence coverage is generally stronger for this domain than for governance or security, so confidence in the presence/absence signals is higher than in areas with a lot of documentation. At the same time, the national mismatch pattern – systems are present, but service management

and staff capacity support are thin – suggests a gap in consolidation between deployment and operational staffing. World Bank analysis links low educational attainment and weak foundational skills to slower digital skills development and cites inadequate funding as a constraint on national human capacity objectives.³⁶

Kenya. Although Kenyan universities generally have ICT units and leadership in place, capacity varies. KENET convenes an annual forum for ICT leaders from Kenyan universities, focusing on cybersecurity, digital infrastructure and workforce development. This indicates existence of a structured peer network for ICT leaders across universities.³⁷

KENET's 2022–23 core data survey reports a median of three “critical” ICT staff per university and one per tertiary college. Many colleges reported having no full-time ICT personnel. The same survey found that over 50% of ICT staff were in end-user support roles rather than specialised system or network administration. It was noted that institutions could reorganise ICT staff budgets to hire more technical experts, as ICT salary expenditure often exceeded internet spending. Retention constraints were documented, with higher private-sector salaries making it difficult for universities to retain skilled ICT personnel.³⁸

Uganda. The higher education ICT workforce is described as being in a state of stratification, with “robust but overstretched” ICT setups in the public sector and “fragile and underdeveloped” capacity in many private institutions. Both public and private institutions are said to be facing shortfalls in continuous training, with a reliance on librarians for

basic ICT literacy workshops. One system administrator attributes stable bandwidth to RENU, as well as to training and advisory support from NITA-U. RENU reports having trained over 2,500 ICT personnel among its member institutions. However, the same body of evidence notes that many smaller or private institutions have been less engaged in these networks.^{39,40}

Rwanda. The ICT Department at the University of Rwanda is led by a Chief Information Officer and comprises staff in various specialised roles.⁴¹ A private university example describes the Directorate of ICT & Online Teaching at UNILAK as organised into sub-teams covering different roles.⁴² Conversely, a case study states that the University of Rwanda purchased enterprise software that it lacked the capacity to fully utilise and remains dependent on the vendor for changes.⁴³ The same account highlights gaps in operational control, as well as a lack of proper backup and security measures in the server room. Having re-established RwEdNet, the Rwandan government is now promoting the establishment of shared services, including a common disaster recovery platform for institutions.¹²

Comparative positioning

Kenya is Developing because evidence documents sector coordination via KENET, as well as modest staffing depth, a support-weighted skill mix and documented training pathways and retention constraints.

36 World Bank. 2022. Somalia Digital Economy Diagnostic

37 <https://mnu.ac.ke/transforming-learning-research-and-working-environments-using-ict/>

38 https://ereadiness.kenet.or.ke/sites/default/files/ctools/2022/Annual_Core_Data_Survey_Report_2022_2023.pdf

39 The Role of RENU and NITA-U in Providing Infrastructure and Online Access in Ugandan Higher Education <https://tojet.net/articles/v24i4/24415.pdf>

40 <https://renu.ac.ug/capacity-building/>

41 <https://ur.ac.rw/?-ICT-Department->

42 <https://site.unilak.ac.rw/directorate-of-ict/>

43 <https://www.ktpress.rw/2025/07/university-of-rwanda-bought-expensive-software-it-has-no-capacity-to-use-for-14-years/>

Uganda is Developing because evidence documents the presence of structured ICT units in a flagship public university, as well as widespread staffing and training capacity constraints, particularly in private institutions, and uneven engagement with shared support networks.

Rwanda is Developing because evidence documents specialised ICT organisational structures in leading public and private institutions, as well as government-backed enablement. However, it also documents vendor dependence and operational control gaps, which signal the ongoing consolidation of internal expertise and execution practices.

Somalia is Emerging in this domain, despite the domain being positioned as a relative national strength. The evidence qualifier cautions this often reflects “structure-on-paper” and coexists with thin staff-capacity support for systems nationwide.

Key explanatory factors

The maturity of NRENs supports workforce development, with KENET and RENU documenting capacity-building programmes and peer learning that can strengthen campus ICT teams. The continuity of shared support is important, given that Rwanda’s NREN is reported to have collapsed in 2018 and restarted in 2024, which has had an impact on learning and services across the sector.^{12,19,21}

Labour-market pressures affect retention, with private-sector salary dynamics documented as pulling skilled personnel away from university ICT units. Cross-country comparisons are also shaped by definitional differences, such as KENET’s definition of “critical ICT staff”.²

Policy commitment and coordination influence the professionalisation of ICT, with Rwanda’s strategic focus on developing ICT capacity linked to government-backed initiatives.

In contrast, Uganda’s evidence base points to weaker policy mandates for ICT staffing across institutions, which

contributes to uneven capacity between public flagship institutions and many private providers.^{38,39}

5.3.4 Governance and planning

Somali HEIs exhibit foundational ICT governance capacity, with formal digital strategies or ICT master plans largely absent or only in the early stages of development across the surveyed universities. Decision-making is typically ad hoc, with limited evidence of dedicated ICT governance bodies, executive-level committees or CIO-type roles driving institutional coordination. Where basic ICT policies exist (e.g. acceptable use or security policies), implementation is weak, as evidenced by a lack of ICT security plans and awareness in recent benchmarking work. Leadership attention to ICT remains limited and not institutionalised, as reflected by the low management awareness scores reported in one benchmark (approximately 0.76 on a scale of 0–3). ICT planning is rarely systematically linked to budgeting, which contributes to a reactive, donor-driven approach to investment rather than execution based on a plan.

Kenya’s universities have stronger foundations in governance and planning, which are reinforced by accreditation requirements that mandate documented institutional policies, including an ICT policy, for both public and private universities.⁴⁴ Sector evidence indicates progress in the maturity of institutional ICT strategies over time. Earlier regional survey findings placed Kenya at an average Stage 2.2 (out of 4) in “Institutional ICT Strategy”, which is consistent with the widespread establishment of ICT departments and some strategic planning. Private universities were reported to have a better ICT strategy than public ones in that survey period, which suggests that the strategy had spread beyond the public sector even at that stage.² More recently, KENET has held annual ICT Directors’ Forums, including a gathering of over 90 ICT directors in 2023, to promote the alignment of IT strategies with institutional goals, financing and operational priorities (e.g. cybersecurity,

44 Kenya Commission for University Education, <https://www.scribd.com/presentation/779658782/COMMISSION-FOR-UNIVERSITY-EDUCATION>

ERP systems and campus networks).⁴⁵

Uganda's governance maturity is more uneven, with a clearer divide between well-established public universities and smaller private institutions. Regulatory minimum standards require universities to have ICT policies and related strategies, which support the formal presence of governance artefacts in both public and private institutions.⁴⁶ Makerere University's ICT Strategic Plan (2020–2030) illustrates the depth of planning possible within flagship public institutions, as it aligns technology initiatives with the institutional mission and long-term objectives.⁴⁷ Regional survey findings placed Ugandan universities at an average Stage 2.1 in ICT strategy.² This is consistent with the presence of defined ICT departments and champions, but there is incomplete integration into the broader institutional strategy. Case-study evidence suggests that many smaller private universities remain closer to the “Emerging” stage. This is characterised by minimal ICT staff, a limited strategic mandate and a reliance on ad hoc decisions, despite the nominal presence of policy.³⁹ RENU's emerging capacity-building role is illustrated by knowledge-sharing engagements, such as Ndejje University ICT staff visiting RENU for ICT knowledge exchange linked to institutional operations and governance learning.⁴⁸

Rwanda's higher education ICT governance is shaped by a strong, centralised national policy environment and a “very strong policy and strategy framework” for integrating ICT into education.⁴⁹ UR, which consolidates much of the public tertiary system, operates with a unified ICT governance structure,

supported by an ICT policy and a multi-year ICT master plan. This strengthens standardisation and oversight across colleges.^{50,51} RwEdNet issues affected the capacity for inter-institutional coordination during the hiatus.¹² There are fewer private universities, which are subject to accreditation oversight. However, available evidence suggests that their capacity varies and may not match that of the UR.⁵²

Comparative positioning using readiness bands

Somalia is Foundational, with limited institutionalisation of ICT governance structures, few formal strategies, weak policy execution and minimal linkage between planning and budgeting.

Kenya is Developing, with near-universal policy frameworks and governance requirements in place through CUE accreditation, active sector coordination through KENET forums and evidence of universities working to operationalise and update strategy. However, implementation quality and review maturity remain uneven across institutions.^{44,45}

Uganda is Emerging/Developing, reflecting stronger governance maturity among public and flagship universities, with institutionalised ICT directorates and strategic plans. However, execution capacity is weaker and governance is more formalistic in many smaller private universities.^{2,39}

45 <https://www.kenet.or.ke/blog/kenet/kenet-holds-ict-directors-forum-universities-research-institutes-and-teaching-hospitals>

46 <https://www.aku.edu/admissions/Documents/policy-academic-quality-framework-ug-005.pdf>

47 <https://policies.mak.ac.ug/sites/default/files/policies/Makerere-University-ICT-Strategic-Plan-2020-2030.pdf>

48 <https://ndejeuniversity.ac.ug/directorate-for-ict-support-visits-renu-for-ict-knowledge-exchange/>

49 <https://education-profiles.org/sub-saharan-africa/rwanda/~technology>

50 <https://ur.ac.rw/documents/policies/ICT%20Policy.pdf>

51 <https://ur.ac.rw/documents/policies/ICT%20Master%20Plan%20-%20Part%202.pdf>

52 <https://education-profiles.org/sub-saharan-africa/rwanda/~technology>

Rwanda is Developing, reflecting strong national strategic alignment and comparatively mature governance in the public system (especially UR). However, sector-wide uniformity and enabling coordination structures, such as a fully active NREN, are still being rebuilt.^{12,52}

Explanatory factors

Quality assurance mandates have a significant impact on governance readiness by requiring ICT policies and strategies for accreditation, thereby accelerating the institutionalisation process in Kenya and Uganda compared to Somalia.^{44,46}

NRENs can bolster governance and planning by facilitating peer learning, professionalisation forums and benchmarking. KENET provides recurring platforms that promote strategic alignment, while RENU is developing similar capacity-building initiatives alongside its technical services. NREN disruptions can undermine sector coordination as shown by RwEdNet's hiatus.^{11,40,45}

Cross-country comparisons remain directional because the evidence is drawn from different years and document types. Internal variation is substantial, with national positioning often influenced by flagship public or NREN-member institutions. Weaker documentation of smaller private institutions can lead to the public/flagship experience being over-represented in comparative signals.^{2,39}

The distinction between the existence of governance artefacts and their effective implementation is a recurring limitation. Sources more often document the existence of policies and plans than the regular functioning of committees, the regular occurrence of reviews, and the measurable shaping of ICT outcomes by accountability mechanisms.

5.3.5 Financial sustainability

Financing for ICT in higher education in Somalia is largely ad hoc and project-dependent, with few institutions

maintaining dedicated budget lines for ICT. Consequently, ongoing costs such as bandwidth, licensing, power, maintenance and ICT staffing are frequently not covered by stable institutional budgets and only addressed when donor support is available or when disruptions occur. Multi-year ICT financial planning is rare, with limited attention given to equipment refresh cycles and total cost of ownership. Donor-funded assets often become difficult to sustain once initial funding ends, creating “build-neglect” risks.

Kenya. Evidence from Kenyan public universities suggests that annual budget provisions for e-learning and ICT are often inadequate for covering recurring and enabling costs, such as staff training, maintenance, content development, bandwidth and infrastructure. Many ICT and e-learning initiatives have depended heavily on donor funding and ICT has not been consistently prioritised in the internal budgets of some institutions.⁵³ KENET's aggregation and cost-sharing model is presented as a key sustainability lever, offering subsidised connectivity and related services to member institutions under a structured fee model. KENET's strategic planning has also recognised limitations in cost recovery and explores efforts to diversify income and strengthen the network's business model. Even under subsidised pricing, however, affordability constraints relative to bandwidth demand are reported, and sustainability signals are weaker for smaller or newer institutions outside the KENET ecosystem.⁵⁴

Uganda. The country's sustainability signals are strongly influenced by the reported impact of RENU on recurrent connectivity costs. This includes a decline in the price of international bandwidth for universities, which fell from over \$1,100 per Mbps/month in 2010 to around \$5 per Mbps/month by 2020.²³ Makerere University reports that these reductions enabled major capacity gains within a stable annual bandwidth budget, shifting from 68 Mbps to around 1.3 Gbps via RENU procurement.⁴⁷ Regional research also cautions that e-learning initiatives in East

53 <https://www.studocu.com/row/document/kisii-university/curriculum-development/challenges-of-implementing-e-learning-in-universities/86221644>

54 <https://www.kenet.or.ke/sites/default/files/kenetstrategicplan.pdf>

African universities often face failure risks linked to financial constraints and short-term project dependence. This implies persistent funding gaps for refresh cycles, training and content beyond the “pipes”.⁵³

Rwanda. The country’s model is characterised by the government’s strong involvement, including the operation of RwEdNet as a unit within the Ministry of Education. This enables direct public funding and institutional anchoring.¹² At the institutional level, UR’s ICT master planning explicitly anticipates blended financing from internal mobilisation, the government, the private sector and international development partners.⁵⁵ Rwanda’s public-sector ICT investments are predominantly government-funded.^{56, 57}

Comparative positioning using readiness bands

Somalia is Foundational, based on Chapter 5’s synthesis of the limited institutionalisation of ICT financing practices, and the high fragility of funding arrangements.

Kenya is Developing for mainstream public universities and KENET-linked institutions, reflecting the partial institutionalisation of ICT budget mechanisms and the stabilising effect of NREN cost-sharing. However, donor dependence and financing inadequacy in e-learning narratives are also noted.⁵³

Uganda is Emerging/Developing. Among RENU-connected public institutions, there are stronger signals of development, given evidence of recurrent budgeting and structural cost reductions. However, there is continuing reliance on external project financing for wider e-learning enablement, based on regional experience.^{23,53}

Rwanda is High Developing, approaching Established. Here, centralised public financing and programme rollouts provide more predictable support for connectivity and educational ICT. However, large upgrades may still be funded through structured public financing and external partner arrangements.^{12,57}

Explanatory factors

Differences in sustainability are closely linked to the commitment and modality of government funding, with Rwanda’s centrally supported education network model contrasting with the greater budgeting responsibility at institution level in Kenya and Uganda. The maturity of NREN cost-sharing determines what institutions can sustain from operating budgets. KENET and RENU are described as mechanisms that reduce unit costs and enable subscription-based recurrent provision.^{23,53}

A recurring theme is striking the right balance between donor-funded capital inputs and domestic recurrent coverage. This is because evidence from the region highlights the constraints of internal budgeting for e-learning, as well as the risks involved when training, maintenance, content and refresh cycles are not fully absorbed. System structure also affects pooling and procurement. Rwanda’s government-led rollouts enable coordinated financing and bulk provisioning through RwEdNet programmes.¹²

Comparability remains limited because key indicators are based on different years and types of evidence (e.g. institutional studies, strategic plans and programme reports) rather than a harmonised budget metric for all countries.

55 <https://ur.ac.rw/documents/policies/ICT%20Master%20Plan%20-%20Part%202.pdf>

56 https://www.minecofin.gov.rw/fileadmin/user_upload/Minecofin/Announcements/ICT.pdf

57 <https://www.minecofin.gov.rw/news-detail/smart-education-project-to-receive-frw-30-billion-financing-boost>

5.3.6 Data security

Somalia's universities have very limited formal data security governance. Chapter 5 reveals that few institutions have dedicated cybersecurity or data protection policies, and that access controls and backups are implemented ad hoc, often only on flagship campuses. Physical server security and disaster recovery planning are sporadic. In practice, even where policies exist, they tend to be incomplete or unenforced, and staff receive little security training or guidance on how to respond to incidents. Overall, Somalia's higher education (HE) data security is at a foundational level: basic controls (e.g. some backup routines) exist here and there, but comprehensive governance and regular audits are absent (coverage is mainly among public and SomaliREN-member universities).

Kenya. The country's higher education security environment benefits from both NREN-enabled services and a national legal framework for data protection. KENET operates KENET-CERT and collaborates with Kenya's national CERT to support incident detection and response for universities. KENET also provides a range of connectivity services, including eduroam Wi-Fi roaming, email filtering, shared hosting and other shared services that can reinforce the security of its member institutions. KENET also offers structured cyber security training courses aimed at campus ICT staff, strengthening skills and awareness where participation is sustained. At the national level, Kenya's 2019 Data Protection Act applies to data controllers and processors, and the Office of the Data Protection Commissioner (ODPC) has issued education-sector guidance on compliance expectations. The ODPC guidance advises educational institutions to publish privacy notices and establish procedures related to breach handling and data processing practices.^{58,59,60,61}

Uganda. RENU operates a CERT, which provides identity and incident response services to strengthen access control and the coordinated handling of security events for its member institutions. It also links with national and regional CERT ecosystems for alert sharing and coordination. RENU established the RENU Identity Federation (RIF) in 2016 and joined eduGAIN in 2018, enabling participating universities to access services and research resources federated across institutions. At the national level, Uganda enacted the Personal Data Protection Act in 2019 and published a National Cybersecurity Strategy for the period 2022–2026. The available narrative indicates that awareness-building is growing through engagements such as webinars for campus ICT staff. However, the formalisation of institutional policies and incident plans remains uneven, especially among newer private institutions.^{62,63}

Rwanda. The country's higher education security environment is shaped by a robust national cybersecurity framework and an up-to-date data protection regime. Rwanda has a Data Protection Law (No. 058/2021) from 2021 and a National Cyber Security Authority, established in 2017, which issues minimum cybersecurity standards for public institutions. In October 2025, Rwanda launched a Cybersecurity Centre of Excellence (CyberHub) at UR's College of Science and Technology, supporting training and professional development in cybersecurity and data protection. Rwanda has also promulgated a five-year National Cybersecurity Strategy (2024–2029), which includes plans to build sector CSIRTs and integrate cybersecurity into education and the broader economy. However, RwEdNet shared services are described as being in their infancy compared to those in Kenya or Uganda. The narrative indicates that Rwanda has not publicly joined eduGAIN and that institutions may therefore rely

- 58 KENET CERT <https://cert.kenet.or.ke/>
59 <https://www.kenet.or.ke/kenet-training>
60 <https://www.kenet.or.ke/content/kenet-connectivity-bundled-services-0>
61 <https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-for-the-Education-Sector.pdf>
62 RENU-CERT, <https://cert.renu.ac.ug/>
63 <https://nordu.net/renu-identity-federation-joins-edugain/>

more on national structures for incident response and awareness, while NREN-enabled shared services mature.^{64,65}

Comparative positioning using readiness bands

Somalia is Foundational, reflecting its limited formal security governance, patchy controls and minimal institutionalisation of incident readiness, as summarised in Chapter 5.

Kenya is Developing, with its maturity supported by national data protection guidance, active services provided by the NREN, such as KENET-CERT, and structured training. However, it is recognised that smaller institutions may lag behind and that institutionalisation is still consolidating.

Uganda is Developing, supported by a RENU-backed identity federation and incident coordination via RENU-CERT, as well as a national cybersecurity strategy framework. However, uneven uptake is acknowledged beyond flagship and RENU-connected institutions.

Rwanda is Developing. This reflects its strong national standards environment and recent capacity-building initiatives, such as CyberHub. However, it is noted that NREN shared services are still in their infancy and coordination structures are still growing.

Explanatory factors

A primary driver is the presence and enforcement of national legal and standards frameworks, which can compel the formalisation of institutional privacy practices, breach-handling procedures and baseline governance expectations.^{61,64}

NREN and CERT ecosystems can enhance sector preparedness by offering shared services, coordinated incident response and training that smaller institutions might struggle to maintain independently at scale.^{58,62,63} Federated identity and inter-federation participation (e.g. eduGAIN) can reinforce consistent access management practices and reduce fragmented credential handling across institutions where adoption is widespread.⁶³

National-level capacity-building investments, such as Rwanda's CyberHub, support skills pipelines and can accelerate institutional capability when linked to policy mandates and operational guidance.^{64,65}

Comparability remains directional because much of the available evidence is drawn from agency guidance, NREN service pages and programme announcements, which do not necessarily provide uniform campus-level adoption measures across all public and private institutions. Where the evidence is strongest for NREN members and flagship universities, band placement should be considered an indication of typical institutional conditions rather than a guarantee of consistent maturity across all tertiary providers.

64 <https://cyber.gov.rw/documentation/>

65 <https://cyber.gov.rw/updates/article/ncsa-launches-cyberhub-to-boost-cybersecurity-skills-and-innovation/>

6 AI and Emerging Technologies

This domain examines the awareness of, early adoption of, and governance of artificial intelligence (AI) and related emerging technologies within higher education institutions. Rather than focusing on mature or large-scale deployment, it considers whether institutions have begun to engage with AI in a structured manner through policy guidance, experimentation, and capacity-building. This domain is exploratory and forward-looking. Findings are intended to inform sequencing and risk-aware planning rather than to assess readiness.

The assessment considers the existence and scope of institutional strategies or formal guidance on AI use, including the areas covered and how ethical, academic and operational considerations are addressed. These indicators provide insight into whether AI is being approached proactively within an institutional framework.

The institutional use of AI tools and platforms is evaluated across core functional areas, including teaching and learning, research, administration, and student services. The indicators capture the extent to which AI applications are in use and the range of activities they support, recognising that adoption is likely to be uneven and exploratory.

The domain also examines institutional efforts to raise awareness of, and build capacity in relation to, AI. Indicators assess whether training or awareness-raising activities have been provided for staff or students, reflecting initial steps towards the informed and responsible use of AI technologies.

Finally, the assessment considers access to computing resources suitable for AI and machine learning, including hardware, cloud-based services and shared infrastructure. These indicators provide insight into the technical feasibility of more advanced AI applications in future.

6.1 Current Awareness and Experimentation

Although reported AI activity is present in a substantial minority of Somali higher HEIs, the pattern is best interpreted as early experimentation rather than institutional adoption. **40% of surveyed institutions report using AI tools or platforms to some extent.** Table 34 includes the personal use of general-purpose tools (e.g. text generation, translation and summarisation) by individual staff or students, even in the absence of institutional endorsement, policy or formal deployment. Reported AI activity therefore reflects exposure and informal practice rather than verified institutional integration.

Alongside reported use, **55%** of institutions indicate that they provide AI-related training or awareness activities. These activities were captured through a yes/no/don't know question and should be interpreted as raising awareness rather than evidence of structured capacity development. The sequencing reported by institutions suggests that training or awareness activities commonly occurred before the reported use of AI, which is consistent with the early stages of sensitisation and experimentation.

Table 34: AI presence and baseline awareness signals

Indicator	Proportion	Comment
Institutions reporting any use of AI tools or platforms	40%	
Institutions providing AI-related training or awareness activities	55%	

Among institutions that report AI use, applications span multiple functional areas rather than concentrating in a single domain. Table 35 shows that reported use is most commonly associated with

teaching and learning (38%) and research (35%), followed by administration (31%). AI use is rarely reported in library services (4%) or cybersecurity (6%). As this was a multiple-choice question asked only of institutions using AI, these figures indicate the distribution of reported usage areas among adopters, rather than system-wide prevalence.

Table 35: Areas where AI use is reported (among institutions reporting any AI use)

Indicator	Proportion	Observation
Teaching and learning	38%	
Research	35%	
Administration	31%	
Library services	4%	
Cybersecurity	6%	

The distribution of AI usage across teaching, research and administration suggests that it is currently being used primarily as a flexible, general-purpose support tool rather than as an institutionally implemented platform embedded in formal workflows. The assessment does not distinguish between routine use and pilot schemes, nor between individual experimentation and deployment at unit level. Consequently, reported AI use should be interpreted as indicative of emerging activity and experimentation, with limited evidence of standardised institutional adoption at this stage.

Across institutions, the reported pattern is consistent with informal uptake driven by individual initiative, often enabled through consumer tools and personal accounts, rather than structured institutional programmes. Where institutional awareness activities exist, they appear to function as introductory sensitisation rather than as formal implementation mechanisms. This provides an early baseline: AI is present in practice, but activity remains uneven and only partially visible through institutional systems and documentation.

6.2 Readiness Gaps and Risks

There has been a reported increase in AI activity in Somali HEIs ahead of the institutional conditions needed for its safe, consistent and scalable use. The baseline evidence suggests **exposure without safeguards**. While AI tools may be used informally, institutional frameworks for governance, capacity building and appropriate infrastructure are limited.

Formal governance signals are scarce. Only **18% of institutions report having a formal AI strategy or institutional guidance**. Where institutions report any form of AI strategy, the most commonly cited areas remain limited in scope. AI in teaching and learning and AI in research are reported by around one-fifth of institutions (20%), while the ethical use of AI and AI training for staff and students are less frequently reported. The weakest coverage is for operational risk controls, including risk management and responsible use (9%), and institutional controls linked to data handling, where data governance and privacy are reported by 11% of institutions. These figures should be interpreted as indicating the presence of stated coverage areas within institutional guidance rather than as evidence of the implementation of ethics frameworks or mature data governance practices.

Table 36: AI governance and institutional capacity signals

Indicator	Proportion
Institutions with a formal AI strategy or guidance	18%
Ethical use of AI	16%
AI in teaching and learning	20%
AI in research	20%
AI in administrative decision-making	11%
Data governance and privacy	11%
AI training for staff and students	16%
Risk management and responsible use	9%
GPU-enabled servers	0%
High-performance computing (HPC)	2%
Cloud-based AI services	8%
Locally deployed AI tools	0%

There are also visible skills and training gaps. Only **16% of institutions reported providing AI training for staff and students as part of their institutional strategy**. This aligns with a broader pattern observed in earlier chapters, where formal ICT training and professional development are not consistently funded or embedded. In practice, limited training increases the likelihood that AI tools will be used without shared norms for responsible use, common standards for academic integrity or consistent awareness of privacy and security risks. While this section does not directly assess AI ethics frameworks, the low prevalence of training and guidance serves as an indicator of limited institutional preparedness for the responsible adoption of AI.

Indicators of infrastructure and computing capacity reinforce the likelihood of dependence on consumer-grade tools and external services. No institutions report having **GPU-enabled servers (0%)**, and only **2% report high-performance computing (HPC) capacity**. **8% of institutions report using cloud-based AI services**, while **none report using locally deployed AI tools**. These results suggest that experimentation in the field of AI is unlikely to be supported by infrastructure managed by institutions and is more likely to rely on external platforms and general-purpose tools accessed through personal or departmental arrangements.

Without institutional AI strategies, limited training and responsible use guidance, and minimal dedicated computing capacity, institutions are more likely to experience fragmented adoption – different tools used in different units with limited oversight – alongside unmanaged risks related to sensitive data handling, procurement and licensing, and uneven access to tools. These risks are structural rather than behavioural; the observed gaps indicate limited institutional mechanisms for standard-setting, capacity-building and accountability as AI use expands.

These findings do not constitute an assessment of AI ethics maturity, nor do they measure data governance quality or compliance. They suggest that the conditions usually associated with the safe and scalable adoption of AI—such as basic institutional guidance, structured training and appropriate computing arrangements—are not yet widely present across Somali HEIs.

6.3 Strategic Positioning

Interest in and experimentation with AI is emerging in Somali HEIs against a backdrop of uneven foundational digital readiness. Evidence from this assessment suggests that, currently, AI functions as an overlay of individual and unit-level experimentation rather than as an integrated institutional capability. Consequently, AI is best understood as a dependent layer that builds on, rather than substitutes for, core digital systems, governance and institutional capacity.

Findings from earlier chapters indicate that many institutions continue to face constraints regarding basic digital infrastructure, internal system integration, governance, staffing, financial sustainability and data security. Against this backdrop, the limited prevalence of formal AI strategies (18%) and the narrow scope of AI-related guidance reinforce the view that the adoption of AI by institutions is outpacing the conditions required for its effective management. Where AI interest exists, it is not yet anchored in stable planning, budgeting or governance frameworks.

Core digital systems and practices, such as reliable connectivity, integrated student and learning systems, defined ICT governance structures, sustainable financing and basic data protection, create an environment in which AI tools can be evaluated, deployed and monitored responsibly. In institutions where these foundations are weak or uneven, AI adoption is more likely to take the form of fragmented tools, parallel workflows and informal data use. This limits potential benefits and increases operational and governance risks.

Evidence from Domains 4–6 supports this sequencing logic. The limited use of learning platforms at programme level, the partial integration of systems, the narrow coverage of ICT budgets, and the uneven practices of security and backup suggest that many institutions are still consolidating their core digital capabilities. In such contexts, AI tools may exacerbate existing disparities rather than address them, particularly where staff capacity, data quality, and institutional oversight are limited.

AI becomes most effective once institutions have achieved a baseline of operational stability and governance maturity. At this stage, it can be used to improve teaching and learning, support administrative efficiency and strengthen research workflows by leveraging institution-managed data and systems. Without these prerequisites, however, AI remains largely opportunistic, driven by individual initiative rather than institutional strategy.

Premature institutional emphasis on AI, in the absence of foundational readiness, risks:

- » Fragmented tool adoption across faculties and units
- » Unmanaged or inconsistent use of institutional and personal data
- » Uneven access to ai tools for staff and students
- » Difficulties in sustaining or scaling ai-related initiatives once initial interest or donor support subsides.

The baseline findings suggest that AI is not a leading driver of digital transformation in Somali HEIs, but rather a capability whose value depends on the strength of underlying digital systems, governance, skills and financial arrangements. This supports an approach of consolidating foundational readiness first, creating the conditions under which AI can be adopted more strategically, equitably and sustainably.

7 Implications for Policy, Investment and Partnerships

This chapter translates the assessment findings into actionable policy, investment and partnership implications. Based on the tier and typology results, it outlines the priorities for different stakeholders – government, SomaliREN and higher education institutions – to strengthen institutional digital capacity in a realistic, staged manner. The chapter progresses from priority actions and targeted pathways to bundled investment packages and delivery models, before moving on to the sustainability and accountability mechanisms required to implement, finance and maintain improvements over time.

7.1 Action Priorities

7.1.1 Sector-wide minimum actions

These are the sector-wide baseline controls and routines that every institution should implement, regardless of their current readiness tier. They do not constitute a ranking and do not assume advanced maturity. Instead, they establish the minimum conditions required to stabilise ICT services, reduce avoidable downtime and data loss, and increase the likelihood of subsequent investments (including shared or pooled investments) delivering sustained capability. The emphasis on this is reinforced by the findings that service disruptions are common and that risk discipline (including restore testing and formal risk assessment) remains uneven across institutions.

- » **Governance and accountability**
- » Implement basic ICT governance and accountable decision-making processes. Appoint a senior ICT focal point with clear authority and establish a lightweight ICT steering function to approve and track priorities. The minimum evidence required is a named accountable lead, governance terms of reference and a simple annual ICT priorities list
- » **Operational discipline and**

documentation

- » Maintain an up-to-date ICT asset inventory and “as-built” documentation. Maintain a basic inventory of devices, servers, endpoints, licences, and critical systems alongside a simple network diagram and topology notes. Minimum evidence: asset register, network diagram and quarterly update log
- » Introduce basic service management (support, maintenance, and escalation). Implement a helpdesk function, log incidents and requests, define escalation procedures and schedule preventive maintenance for core infrastructure. The minimum evidence required is a ticket log/structured register, a maintenance schedule and a monthly summary of the top issues
- » **Reliability baseline: make services usable before expanding**
- » Stabilise power and connectivity for core services before expanding the scope. Prioritise power backup for critical ICT nodes and implement basic redundancy planning for connectivity where feasible. Implement bandwidth management practices to protect priority services. The minimum evidence required is basic uptime tracking, a power backup coverage list and bandwidth management notes
- » **Security, continuity and control of core platforms**
- » Standardise identity and access management for institutional systems. Official accounts should be used, role-based access should be implemented for sensitive systems, and account lifecycle processes should be formalised. The minimum evidence required is an account policy/procedure, a role matrix for key systems and a deprovisioning checklist
- » Implement minimum cybersecurity controls and patch

discipline. Ensure perimeter and endpoint protection, routine patching and simple security logging and review. Minimum evidence: a patch/update schedule, a record of firewall rule responsibilities, and a basic security event log

- » Establish backup and restore testing procedures and a basic continuity plan. Back up critical systems on a defined schedule and keep at least one protected/offsite copy. Test restores periodically. The minimum evidence required is a backup schedule, a retention plan and documented restore test results
- » Clarify ownership of systems and data and implement change control for core platforms. Appoint an owner for each major system and define how data ownership, change approval and integration requests are handled. Minimum evidence required: a list of system owners, a change log and a simple integration roadmap (phased if necessary)
- » **Sustainability and collective alignment**
- » Formalise ICT budgeting and lifecycle planning, including operational expenditure (OpEx). Distinguish between recurring costs and one-time investments and define refresh cycles. Provide a minimum of the following evidence: an annual ICT budget summary; a list of operating expenses (e.g. bandwidth, licences, maintenance); and a basic refresh plan
- » Develop a practical ICT capacity development plan linked to operational needs. Assess skills against required functions and prioritise short training/certification pathways and peer learning. The minimum evidence required is a skills matrix, an annual training plan and a participation record
- » Introduce baseline data governance and privacy practices. Define sensitive data, storage locations, access rules, retention periods and incident reporting procedures. The minimum evidence required is data classification notes, retention rules for key datasets and an incident

reporting protocol

- » Adopt shared standards and collective approaches where these reduce costs and risks (including SomaliREN, where feasible). Align with common baselines for networking, security, hosting, and interoperability. Use shared services or pooled procurement models where appropriate. Minimum evidence: documented adopted standards and a shortlist of services suited to shared delivery

These actions are intentionally sector-wide minimums. They can be implemented immediately, even in low-capacity settings, and they create the conditions for quicker progress across tiers, stronger partnerships and more sustainable investment outcomes.

7.1.2 Differentiated pathways by readiness tier

Readiness tiers are most useful when treated as sequencing guides rather than performance labels. As the national picture is best understood as predominantly Tier 1–3 (with Tier 3 the highest tier observed in the dataset), the pathways below prioritise staged, realistic improvements over “leapfrogging” to advanced solutions. Each pathway sets out:

- » A practical target state for 12–18 months’ time;
- » The small number of moves most likely to move an institution forward;
- » The constraints that typically slow progress; and
- » The kinds of support that would be most helpful from the government, SomaliREN and partners.

While institutions within a tier can differ significantly (addressed further through typologies), the tier pathways provide a common planning baseline.

Tier 1 – Foundational: Establish a stable institutional baseline

- » **12–18 month target state:** Core ICT services are stabilised and governable, with basic connectivity and campus networking functioning reliably for priority services. Minimum operational routines exist for support, maintenance and backups, and governance and budgeting mechanisms are beginning

to form.

» **Priority moves:**

- » Implement basic governance (appoint an ICT lead, establish a lightweight steering group and develop a simple ICT priorities plan).
- » Stabilise reliability by implementing power backup for ICT nodes, basic network hygiene and uptime tracking.
- » Implement minimum security and backup discipline (access control basics, patching routine and restore testing).
- » Create foundational documentation such as an asset register, network diagram and system owner list.
- » Establish a visible ICT budget line or equivalent mechanism for recurrent costs.

» **Common constraints:**

- Fragmented decision-making
- Limited documentation
- Insufficient recurrent funding
- Dependency on a small number of staff or external technicians.

» **Support required:**

- Targeted technical assistance (e.g. templates, coaching and baseline standards)
- Shared procurement support (to reduce cost and vendor fragmentation)
- Small catalytic funding tied to minimum controls (especially for power/network stabilisation and backup/security basics).

Tier 2 – Emerging: Consolidate and formalise existing processes

- » **12–18 month target state:** Operational capability is converted into repeatable institutional practice. Governance and planning become functional, rather than symbolic. Security controls become more comprehensive and financing begins to match the true cost of running services.

» **Priority moves:**

- » Formalise governance and planning into execution routines (work plans, responsibilities and review cadences).
- » Strengthen financial sustainability by separating CapEx/OpEx, defining recurring cost coverage and beginning lifecycle planning.

- » Improve operational consistency (helpdesk discipline, preventive maintenance and documentation updates).
- » Transition from isolated controls to a security posture (access control, incident handling and monitoring fundamentals, rather than backups alone).
- » Rationalise systems by reducing duplication, clarifying system ownership and beginning integration planning.

» **Common constraints:**

- “Patchy institutionalisation” (some policies and systems exist but are not enforced)
- Uneven coverage across campuses
- Recurrent cost pressure (e.g. bandwidth, licences, staffing, power).

» **Support required:**

- Shared service options (where feasible), with clear onboarding requirements
- Governance and finance coaching (budgeting and cost recovery)
- Procurement frameworks that reduce vendor fragmentation and improve service levels.

Tier 3 – Developing: Make the institutional form work in practice

- » **12–18 month target state:** Institutions move from compliance signals to reliable execution. Systems are used consistently; controls operate as intended and performance is managed through measurable service standards and continuous improvement routines.

» **Priority moves:**

- » Strengthen execution capacity (define service standards, measure uptime/response times, enforce change control).
- » Consolidate institutional systems and integration (interoperability, data quality and clarity of roles across registrar, finance, academics and ICT).
- » Mature security and risk management (incident response, periodic audits, privileged access management and tested

continuity).

- » Operations should be professionalised (IT service management, asset lifecycle management, and vendor performance management).
- » Staffing should be aligned to functions (network, systems, security and support) rather than generic ICT roles.

» **Common constraints:**

- “Operational drag” despite the presence of policies – systems exist but are inconsistently managed
- Institutional complexity increases, making coordination more difficult
- Security maturity may lag behind service expansion.

» **Support required:**

- Advanced technical assistance (integration architecture and security hardening)
- Structured peer learning across comparable institutions
- Shared platforms that reduce overhead costs (identity management, hosting and monitoring), where governance and readiness allow.

These tier pathways provide a default sequencing logic for implementation planning. They should be applied flexibly, recognising that institutions may require different starting points within the same tier, depending on their dominant constraint profile. This issue is addressed directly in the typology-based targeting in the next section.

7.1.3 Typology-sensitive targeting within tiers

Readiness tiers indicate an institution's overall progress (Tiers 1–3 were observed in this assessment), while typologies clarify the dominant constraint profile within a tier and therefore the most effective sequencing and support. In practice, institutions within the same tier often require different interventions because their binding constraints are in different areas, such as governance, execution discipline, infrastructure reliability, systems integration, or financial sustainability. Typology-sensitive

targeting helps avoid a one-size-fits-all “tier package” approach, enabling implementers to provide the appropriate combination of investments, technical assistance and change management to the relevant institutions.

Where the binding constraint is structural (e.g. cost/reliability of upstream connectivity or shared platform requirements), typology-sensitive targeting should prioritise collective solutions (such as pooled procurement and shared services via SomaliREN) over isolated fixes for each campus.

Typologies are used here as an implementation lens, not as a second ranking. They help to:

- » Identify the binding constraint that is limiting progress within a tier
- » Adjust sequencing by distinguishing between prerequisites and accelerators
- » Form peer-learning cohorts that share comparable bottlenecks to improve the relevance of shared tools and support
- » Align support with evidence quality by distinguishing between genuinely absent capabilities and those that are simply not yet documented or verified
- » Distinguish between constraints that can be resolved by the institution and those that require pooled delivery at system level (e.g. shared connectivity, platforms and procurement).

Operationally, the targeting rule is straightforward: Use the tier to set ambition and time horizon, and use the typology to choose the entry point, sequencing and support intensity.

Table 37 summarises this logic in a practical matrix. It links each typology to its binding constraint and outlines priorities and common missteps to avoid, as well as a small set of fast indicators that can be tracked over the first 3–6 months to confirm that implementation is moving in the right direction.

Table 37: Typology-to-intervention targeting matrix

Typology (within tier)	Binding constraint	What to prioritise (intervention emphasis)	What to avoid	Fast indicators of progress (3–6 months)
T1-A: Operational Presence, Institutional Void	Capability exists but is not institutionalised (weak governance, documentation, controls, budgeting).	- Minimum governance scaffold (accountable ICT lead + steering cadence) - Basic policies/SOPs, asset register + network diagram - Backup/restore discipline - Visible ICT budget recognition - Basic service management routine (issue log + escalation + monthly review)	- Buying new systems or expanding scope before controls/ routines exist “Policy writing” without execution routines.	- Named accountable ICT lead - Basic ICT priorities plan - Asset register + network diagram produced - Backup schedule + at least one successful restore test - Helpdesk/issue log active + first monthly review held
T1-B: Infrastructure-Forward, Governance-Constrained	Infrastructure is present but decision-making and standards are weak; growth is ad hoc.	- Standardisation + governance discipline: procurement standards - Network/service baselines - Change control, basic performance tracking (uptime/incidents) - Security minimums sized to current footprint - Default to shared standards/procurement frameworks (incl. pooled procurement where feasible)”	- Additional infrastructure rollouts that increase complexity - Vendor-by-vendor fragmentation “One-off upgrades” without operating model.	- Basic standards adopted (network/ security) - Change log initiated - Uptime/incident tracking in place - Recurring outage frequency/duration tracked and trending down (baseline + month 3) - Vendor/service inventory consolidated.
T1-C: Fragmented Readiness	Readiness is uneven and incoherent across domains/ campuses; weak coordination.	- Coherence bundle: (i) governance cadence, (ii) service log + escalation, (iii) asset/network documentation, (iv) backup/restore discipline - Establish a single institutional roadmap and minimal common practices across campuses.	- Multi-track “everything at once” - Parallel systems per unit - Jumping to integration/AI initiatives.	- Single institutional ICT roadmap agreed - Common minimum practices adopted across campuses (accounts + backup + incident logging) - Consolidated assets register across campuses - Basic helpdesk log covering main services - Fewer duplicated tools/ platforms.

T2-A: Operations-Led with Sustainability Gaps	Services run, but financing and lifecycle planning lag; risk of deterioration.	• Budget formalisation (CapEx/OpEx separation) • Lifecycle/refresh planning • Cost controls (aggregate procurement, rationalise licensing) • Service catalogue and cost drivers • Vendor performance management • Renewals calendar (bandwidth/licences/hosting) and approved OpEx coverage plan	• Expanding platforms without recurrent cost coverage • Adopting high-licensing solutions without exit plans • Under-budgeting maintenance/bandwidth.	• ICT budget line or equivalent formalised • OpEx list (bandwidth/licenses/power/maintenance) documented • Refresh plan drafted • Procurement/contract register created • Maintenance schedule executed for critical nodes + fewer repeat incidents logged for the same root causes
T2-B: Governance-Led, Implementation Catch-Up	Formal governance exists, but execution/implementation capacity and/or infrastructure reliability lags behind intent	• Convert plans into routines (workplans, owners, review cadence) • Operational stabilisation (network/power reliability, monitoring, preventive maintenance) • Minimum IT service management discipline (ticketing, SLAs/service targets, change control) • Sequence: stabilise reliability and service routines before expanding platforms	• More policies/committees without execution mechanics • New systems that increase operational load before reliability improves	• Workplan cadence operating (monthly review) • Ticket log + response targets used • Uptime/incident metrics tracked for priority services • Preventive maintenance schedule initiated • Uptime baseline established for 2–3 priority services
T2-C: Uneven Advancement	Progress exists but is lopsided; weakest domain drags overall readiness.	• Target the weakest domains with “catch-up bundles” (often governance, security, sustainability, or integration discipline) • Use structured sequencing and peer learning to standardise practice • Prioritise the weakest domain even if it is “less visible” (governance, OpEx, security)	• Treating the institution as uniformly mature • Investing only where it’s already strong • Adding new platforms while foundational gaps persist.	• Weakest domain shows measurable improvement (e.g., security controls implemented, budgeting formalised, or service management adopted) • Minimum baselines implemented across all campuses (same incident log, backup routine, and account practices) • Clearer system ownership and reporting cadence.

T3-A: Broadly Balanced, Selective Gaps	One or two specific lagging domains block transition.	- Targeted “finish-line” interventions: close the specific gap(s) with defined deliverables (e.g., security hardening, sustainability plan, integration improvements) - Institutionalise continuous improvement - Performance management: service targets and vendor performance review cadence	- Broad restructuring - Replacing systems unnecessarily - Spreading resources thin across all domains.	- Lagging domain shows closed-loop completion (e.g., Restore testing completed and scheduled (e.g., quarterly) with documented results, Integration milestone achieved, OpEx funding secured) - Performance metrics stabilise - Internal review/checklist confirms closure of the identified gap(s) with evidence
--	--	---	--	---

7.2 Investment Packages and Sequencing

This section translates the priority actions and tier/typology logic into a small set of coherent investment packages that can be planned and financed together. Packaging reduces fragmentation and avoids the common failure mode of upgrading individual systems or infrastructure components in the absence of the enabling conditions required for sustained performance. Table 38 provides the primary definition of each package, including its core scope, explicit exclusions, and minimum prerequisites, as well as key sustainability considerations affecting affordability and long-term operation. The short subsections that follow briefly clarify the intent of each package and emphasise the importance of practical implementation.

Several package elements, particularly those relating to shared platforms, baseline security tooling and connectivity procurement, are designed to be delivered through collective mechanisms (including SomaliREN and pooled procurement). This reduces duplication, improves consistency and lowers unit costs. Given the national profile of the institutions involved (predominantly Tier 1–Tier 3, with Tier 3 being the highest tier observed), the packages are structured to support a staged progression from stabilisation to institutionalisation. However, they still allow for more advanced investments where the necessary readiness and safeguards are in place.

The packages are designed to be sequenced, not deployed as a single national “shopping list”. Sequencing matters because progress depends on dependencies across domains. For example, reliable power and campus networking must be established before core systems and platforms can be scaled up, identity and access controls must be in place before sensitive systems can be expanded, and backup, patching, and service management routines must be established before complexity can increase through integration or advanced services. The sequencing guidance that follows provides practical rules for selecting the right starting point by

tier and typology, and for coordinating investments so that early gains are stabilised and later upgrades result in durable institutional capability.

7.2.1 Package A – Foundational Infrastructure and Reliability

Package A establishes the minimum infrastructure and reliability conditions required for digital systems to be usable and supportable, and to be capable of scaling up. Its focus is on stabilising the foundations that underpin all other packages, including ensuring the integrity and coverage of the campus network in priority areas, providing reliable internet connectivity and protecting critical ICT nodes. For many Tier 1 and Tier 2 institutions, and for Tier 3 institutions with residual reliability gaps, this is the most binding prerequisite; without it, investments in platforms, integration, and advanced services will typically underperform or fail.

Package A will include targeted improvements to the campus backbone and switching, priority-zone Wi-Fi, and fixes to the structured cabling. It also includes measures to ensure adequate bandwidth and reliable connectivity (including basic redundancy where feasible), power stabilisation for ICT (uninterruptible power supplies (UPS) and backup power arrangements for core nodes), and basic monitoring routines to track uptime and recurring faults. Where cost and reliability of upstream connectivity are the binding constraints, these elements should be planned to align with collective procurement and aggregation options (including SomaliREN/NREN pathways) rather than being addressed on a campus-by-campus basis.

Out of the scope of Package A are universal high-density Wi-Fi coverage as a default first step; large-scale procurement of end-user devices; major enterprise system replacement or integration work (covered elsewhere); and advanced security operations that go beyond the baseline protections required to safely operate the network.

Success is demonstrated through

measurable improvements in uptime and service continuity for priority institutional services, supported by basic monitoring records and maintenance routines that the institution can sustain.

7.2.2 Package B – Shared digital services and core platforms

Package B consolidates a set of shared, reusable digital services which are generally more efficient and sustainable when delivered collectively rather than being replicated by individual institutions. The package focuses on the “common backbone” services that enhance the reliability, security and user experience of multiple institutional systems, particularly where SomaliREN or coordinated consortium arrangements can reduce unit costs, enhance service quality and reinforce standards. In peer systems, NRENs have often been the primary mechanism for scaling these services through pooled demand, shared infrastructure and common standards, thereby enabling faster progress across the sector as a whole.

Package B will include shared or standardised services, including institutional identity and access management (with single sign-on where possible), email and collaboration services, hosting options for core services (centralised, federated or hybrid), backup and recovery platforms, and baseline monitoring and security tools that can be provided as a managed service. It may also include templates and service-level agreements that clarify ownership of services, responsibilities, and performance expectations, as well as procurement frameworks that specifically support the delivery of shared services.

Adoption of Package B should be evidence-based: institutions require minimum readiness, such as reliable local connectivity for users, basic account management, and a first-line support function, and should pair shared services with Package D routines to ensure services remain operational and secure at an institutional level. EARDIP can act as a catalytic platform to finance early onboarding and shared platform development, while establishing sustainable cost-sharing arrangements

for ongoing operations.

Out of the scope of Package B are the replacement of core institutional business systems (e.g. SIS, LMS and finance/HR systems) and major institution-specific integration work (covered under Package C), as well as advanced security operations that go beyond the baseline/managed tooling intended for broad adoption.

Success is demonstrated through: (i) adoption of shared services across a growing number of institutions (e.g. standardised accounts and usage of the shared platform); (ii) operational clarity (service ownership, SLAs and routine service reporting); and (iii) a measurable reduction in duplicated tools and ad hoc platform deployment.

7.2.3 Package C – Institutional systems and integration

Package C strengthens the core institutional applications that facilitate academic delivery and administrative management. Rather than focusing solely on software acquisition, there is an explicit emphasis on integration, interoperability and operating models. The objective is to ensure that key systems (and the processes they support) function reliably from start to finish, with clear ownership, consistent data handling, and scalable, user-facing services.

Package C will involve setting up, consolidating or upgrading core systems, such as the Student Information System (SIS), the Learning Management System (LMS), library systems and repositories, and selected administrative systems (e.g. finance and HR), provided that institutions have the necessary authority and resources. This is accompanied by foundational integration work that reduces duplication and improves workflow continuity. Integration should be incremental and workflow-led, beginning with a few priority processes and datasets. Package C also covers the governance elements required for sustainability, including defined system owners, role-based access, change control, data quality routines, and basic interoperability standards (including APIs or integration middleware, where feasible). SomaliREN can support these

efforts by providing reference standards, templates, and shared technical guidance for interoperability and secure configuration. However, institutional ownership and accountability for core systems remains with Higher Education Institutions (HEIs).

Out of scope for Package C are foundational infrastructure and power stabilisation (Package A), broad shared service platforms such as identity, hosting and backup delivered collectively (Package B) and operational capability building (Package D). These are prerequisites for sustained performance. In practice, Package C should be evidence-gated; it should not be accelerated until the target system(s) have reliable access control and backup/restore testing routines in place.

Success is demonstrated through consistent use of core systems for priority processes (e.g. registration, results, and learning delivery); fewer parallel/manual workarounds and improvements in data quality and integration that are visible (e.g. fewer duplicate records, smoother cross-unit workflows, and more reliable reporting).

7.2.4 Package D – Operations, Capability and Service Management

Package D establishes the institutional operating capacity required to reliably provide ICT services and improve them continuously over time. It focuses on the practical routines, tools, and human capabilities needed to transform infrastructure and systems into reliable services. This reduces reliance on ad hoc troubleshooting and ensures that upgrades remain functional after project support ends. For many institutions, Package D is the difference between “having technology” and “delivering services”. Package D should be implemented alongside Packages A–C from the outset, as reliability upgrades and core systems cannot be sustained without minimum operational, documentation and support routines.

Package D will involve setting up or improving IT service management practices, including helpdesk/ticketing systems, structured logs, incident

and request handling, and escalation pathways. It also covers preventive maintenance routines, systems and network documentation, asset management and lifecycle tracking, basic monitoring practices, and targeted capacity development. This includes creating skills matrices, as well as training and certification pathways that are aligned to the required functions. The package also includes measures to clarify roles and structure workloads, ensuring that critical functions (e.g. networking, systems administration, support and security) are consistently covered. SomaliREN can accelerate the implementation of Package D by using shared templates (standard operating procedures (SOPs), logs and checklists), cohort-based peer learning and coordinated training pathways.

Out of scope for Package D are major capital upgrades of network/power infrastructure (Package A) and large-scale platform replacement or integration projects (Package C), except where small operational tools are required to manage these investments effectively (e.g. ticketing, monitoring and asset management tools).

Success is demonstrated through improved operational performance, including faster issue resolution, fewer recurring faults, documented maintenance and change routines, clearer accountability for services and evidence that the institution can sustain day-to-day operations and incremental improvement without relying on external troubleshooting. Minimum evidence requirements include active incident/ticket logs, completed maintenance records and documented restore tests and change logs.

7.2.5 Package E – AI-ready enablers and responsible innovation

Package E helps institutions adopt AI and other emerging technologies safely and productively by strengthening the conditions that enable responsible innovation. It acknowledges that AI preparedness is not just about acquiring tools, but also about ensuring sufficient data governance, security, operational controls, and decision accountability to manage risk, protect privacy, and generate reliable value from early use cases. In most cases, Package E should only be activated once the minimum requirements under Packages A–D have been met, particularly: (i) stable core services and support routines, (ii) basic identity and access control discipline, (iii) backup and restore routines, and (iv) baseline data governance practices.

Package E will usually contain baseline data governance practices, such as data ownership, classification, retention and access controls. It also includes privacy and security safeguards that are aligned to institutional risk, as well as practical guidance on the acceptable and responsible use of AI in teaching, learning, research and administration. This guidance covers topics such as academic integrity, responsible staff and student use, and rules for handling sensitive institutional data when using external AI services. It also includes a controlled approach to piloting, involving clear problem definition, data readiness checks, defined success metrics, monitoring and evaluation, and explicit scale/stop decisions. Where necessary to ensure the safety of experimentation,

it may include limited enabling choices, such as approved approaches to hosting AI workloads, data storage arrangements and targeted capacity building for leadership and technical teams in the areas of AI risk, procurement and oversight. Sector actors (government and SomaliREN) can support Package E by providing shared guardrails, templates and reference standards, which reduce duplication and help institutions to adopt consistent minimum safeguards.

Out of scope for Package E are large-scale AI deployments without foundational controls, institution-wide automation or decision systems that materially increase risk, and AI investments that bypass minimum requirements for security, data protection and operational sustainability. High-risk uses, such as automated decision-making for admissions, grading, disciplinary actions, staff performance management or financial eligibility, should not be pursued without explicit governance, robust controls and clear accountability mechanisms.

Success is demonstrated through the following: (i) clear institutional guardrails, including roles, policies, and approval pathways for AI use and academic integrity provisions; (ii) improved discipline in handling data and documented risk controls for AI-enabled tools; and (iii) a small number of well-scoped pilots that are transparently evaluated and demonstrate learning and benefits without creating unmanaged security, privacy, or integrity risks.

Table 38: Investment packages definition

Package	Purpose	Includes (core scope)	Explicit exclusions	Minimum prerequisites	Best-fit tiers
A – Foundational infrastructure and reliability	Make digital services usable and supportable by stabilising campus networking, connectivity reliability and power for priority services.	• Campus backbone/switching and structured cabling fixes (priority zones) • Priority-zone Wi-Fi where needed (not universal first step) • Bandwidth adequacy + basic redundancy where feasible • Power protection for critical ICT nodes (UPS/backup power arrangements) • Basic uptime/outage tracking and fault logging	• Universal high-density Wi-Fi as the first step • Large end-user device programmes • Major business system replacement or integration work	• Access to critical ICT spaces and equipment • Basic maintenance ownership and escalation (start Package D routines early) • Authority to manage/standardise network configuration	T1-T2 primary; T3 targeted gap-closure; T4 resilience optimisation (aspirational)
B – Shared digital services and core platforms	Reduce duplication and improve consistency through shared/standardised “backbone” services delivered collectively (SomaliREN/consortia), improving quality and lowering unit costs.	• Identity and access management (SSO where feasible) • Shared email/collaboration options (where adopted) • Hosting options for core services (centralised/federated/hybrid) • Shared backup/recovery platforms • Baseline monitoring/security tooling as a managed service • SLAs/templates and configuration standards for shared services • Procurement frameworks/templates that enable shared service delivery	• Replacing SIS/LMS/ERP core business systems • Heavy institution-specific integration (Package C) • SOC-grade advanced security operations	• Minimum local reliability to consume shared services (basic connectivity + campus network stability) • Account lifecycle discipline and willingness to adopt standards/SLAs (and cost-sharing where applicable) • First-line institutional support function for users/escalation	T2-T3 primary; T1 selective (where minimums met); T4 optimisation/leadership (aspirational)

C – Institutional systems and integration	Strengthen core institutional systems with interoperability and operating model discipline—ensuring end-to-end process reliability, not just software acquisition.	- Establish/upgrade/consolidate SIS/LMS/library and priority admin systems (e.g., finance/HR) where mandated and operable - Incremental, workflow-led integration/interoperability (APIs/middleware where feasible) - System ownership and governance: RBAC, change control, data quality routines, basic interoperability standards	- Foundational infrastructure/power stabilisation (Package A) - Shared platform services best delivered collectively (Package B) - Operations capacity building as the primary focus (Package D)	- Stable connectivity/power for priority services (Package A) - Support routines and capacity in place (Package D) — ticketing/logs, maintenance, documentation discipline - Baseline identity/backup arrangements where applicable (Package B) - Evidence gate for the target system(s): access control + restore testing + operational support ready	T2–T3 primary; T1 limited (single priority workflow only); T4 advanced integration/analytics (aspirational)
D – Operations, capability, and service management	Turn technology into dependable services and sustain gains after projects end through routines, tools, documentation and role coverage.	- Helpdesk/ticketing (or structured logs), incident/request handling and escalation pathways - Preventive maintenance routines; documentation/SOPs; basic monitoring practice - Asset management and lifecycle tracking (inventory, refresh planning inputs) - Skills matrix, training/certification pathways aligned to functions - Role clarity and workload structuring (network, systems, support, security)	- Major CapEx infrastructure upgrades (Package A) - Large-scale platform replacement/integration programmes (Package C) - Non-essential tooling beyond what supports operations	- Leadership commitment to routines, reporting and accountability - Minimum staffing time allocated and roles assigned - Adoption of standard logs/templates (and shared tools where used)	T1–T3 essential; T4 continuous improvement (aspirational)

E – AI-ready enablers and responsible innovation	Enable safe, controlled AI adoption by strengthening data governance, safeguards and pilot discipline; focus on risk-managed value, not tool acquisition.	• Data governance basics (ownership, classification, retention, access controls) • Responsible use guidance + approval pathways (incl. academic integrity and handling of sensitive data with external AI services) • Controlled pilots (problem definition, data readiness checks, monitoring & evaluation, scale/stop decisions) • Limited enabling choices where required (approved hosting/storage approaches for safe experimentation) • Targeted capacity building for leadership/technical teams on AI risk, procurement and oversight	• Large-scale AI deployments without foundational controls • High-risk automation/decision systems without strong governance (e.g., admissions, grading, disciplinary decisions, eligibility determinations) • AI investments that bypass security, data protection and OpEx sustainability	• Minimum safeguards from Packages A–D evidenced (reliability, access control, backup/restore testing, support routines) • Basic data handling discipline and named accountability for AI approvals • Privacy/security safeguards defined for pilot data and tools	T3 primary; T2 selective (low-risk use cases under guardrails); T4 scaling/centre-of-excellence role (aspirational)
--	---	---	---	--	---

Note: The assessment covered Tiers 1–3 only (Tier 3 being the highest). Tier 4 is included here as a long-term aspiration.

7.2.6 Sequencing rules and prerequisites

The packages in Section 7.2 are designed to be combined, but not all deployed at once. In practice, the order in which they are deployed should be guided by a small number of dependency rules. This will protect institutions from premature complexity, ensure that minimum safeguards are in place and stabilise initial progress, ensuring that later upgrades remain sustainable. The following rules provide a pragmatic basis for selecting an entry point and for sequencing the packages over a period of 12–18 months. Where collective delivery reduces costs and fragmentation, the sequencing should also consider shared mechanisms (e.g. SomaliREN and pooled procurement) as well as institution-level actions.

Rule 1: Stabilise reliability before scaling platforms

Where connectivity, campus networking, or power reliability are unstable, Package A is a prerequisite for meaningful progress in Packages B and C. Institutions should prioritise reliability for critical services and priority zones before attempting broad system expansion.

Rule 2: Build operational capacity in parallel with infrastructure upgrades

Package A alone rarely delivers long-lasting improvements unless institutions can operate and maintain the installed equipment. Package D should be initiated early and implemented alongside Package A for Tier 1–2 institutions, and as enabling reinforcement for Tier 3 institutions undertaking upgrades.

Rule 3: Make use of shared services at an early stage if they reduce duplication and strengthen standards

If governance readiness and adoption capacity are in place, Package B can be implemented at an early stage — often alongside Packages A and D — because shared identity, hosting, backup and baseline monitoring reduce duplication and provide a stable foundation for institutional systems. Where the binding constraint is structural, such as cost/quality of connectivity, lack of shared platforms

or vendor fragmentation, shared delivery through SomaliREN or consortium arrangements should be the default approach. However, Package B should not be adopted if institutions cannot meet the minimum operational requirements for account management, basic controls, and defined responsibilities. EARDIP can act as a catalytic platform to finance early onboarding and the development of shared platforms while establishing sustainable cost-sharing for ongoing operations.

Rule 4: Do not expand core institutional systems any faster than the rate at which governance and controls are developed

Implementation of Package C (SIS/LMS and other core systems) should only proceed once the following basic prerequisites are in place:

- » Stable connectivity and power for priority services (A);
- » Minimum operational routines and support capacity (D);
- » Identity/access and backup practices (B), where applicable. This reduces the risk of “system rollout without service delivery” and prevents the accumulation of technical debt.

Rule 5: Integration increases risk and must follow minimum discipline

Systems integration and interoperability work under Package C should only begin once institutions have demonstrated minimum change control, access management, documentation and backup/restore testing. Without these, integration increases the risk of failure and can exacerbate data integrity issues across systems.

Rule 6: AI readiness comes after controls and data discipline

Package E should be considered a later-stage enabler rather than an early-stage substitute for foundational readiness. Institutions should only activate Package E once the following minimum safeguards are in place: stable services (A), operational routines (D), baseline security and access controls, and basic data governance. This

ensures that pilots are controlled, risks are managed, and learning is captured.

Rule 7: Sequence by binding constraint, not aspiration

Entry points should be chosen based on the institution's typology.

- » If the binding constraint is reliability (power, network or connectivity), start with A and D, then add B, then C and finally consider E
- » If the binding constraint is institutionalisation/sustainability, start with D (execution routines and service management), then add targeted B (shared standards/tools), and finally consider C once recurrent cost coverage and controls are in place
- » If the binding constraint is systems fragmentation and weak workflows, prioritise C once minimum stability and operational discipline (A/D) are in place. Use B to reduce duplication where shared services can replace ad hoc solutions.

Rule 8: Prove readiness with evidence before moving to the next package

Progression should be based on practical evidence, not intent. Examples of this include uptime logs and fault trends (A); a functioning helpdesk/ticket log and completed maintenance routines (D); implemented account and access practices, including service ownership and SLA reporting (B); demonstrated system usage and workflow improvements (C); and documented AI guardrails, along with pilot evaluation results (E). This evidence-based approach promotes accountability and safeguards limited resources.

These sequencing rules support a staged implementation approach, whereby early investments produce stable service improvements, later investments deepen capability and integration, and AI-related innovation is pursued only when the foundational conditions for responsible adoption are in place.

7.3 Partnership and Delivery Models

The investment packages set out in Section 7.2 will only translate into sustained institutional capability if they are matched with feasible delivery mechanisms. In the context of higher education in Somalia, delivery models are as important as technology choices because structural constraints, such as limited technical capacity in individual institutions, fragmented procurement, inconsistent standards and weak recurrent funding, often determine whether services remain operational after project support ends.

Similar constraints have been addressed by peer systems through strong National Research and Education Networks (NRENs), which use pooled demand, shared services and sector-level coordination to improve quality and reduce unit costs. SomaliREN could play a similar role by scaling up collective connectivity and shared backbone services while encouraging institutions to adopt common standards and operating practices.

Section 7.3 therefore sets out practical partnership and delivery options, including shared delivery arrangements (7.3.1), market-facing partnerships (7.3.2) and enabling government roles (7.3.3). The intention is not to promote a single model, but rather to clarify which models best suit the different packages, the governance conditions they require and the necessary risk management safeguards. EARDIP should be treated as a time-bound opportunity to catalyse these delivery mechanisms, especially collective connectivity and shared services, so that investment is not fragmented into isolated campus upgrades.

7.3.1 Shared delivery models

Shared delivery models offer a practical solution to two issues identified in the assessment: many institutions encounter similar bottlenecks, and duplicating the same capabilities across numerous institutions is frequently impractical, costly, and challenging to maintain. Shared approaches can reduce unit costs, improve quality through professionalised operations and accelerate standardisation, particularly for services that are common across institutions and benefit from centralised expertise. This chapter presents shared delivery as a set of complementary options that can be implemented via SomaliREN, university consortia or pooled procurement frameworks. These options are not mutually exclusive and can be combined depending on institutional readiness, trust conditions and the package being implemented.

SomaliREN is best suited to delivering “shared backbone” services that multiple institutions require and which demand continuous operational attention. It aligns most strongly with Package B (shared identity and access, email/collaboration options, hosting, backup/recovery and baseline monitoring/security tooling) and can support Package D by providing shared templates, standards, training pathways and operational coaching. Where infrastructure constraints are limiting, SomaliREN can also coordinate collective approaches under Package A, including demand aggregation for connectivity, definition of service levels, and technical guidance on standards and redundancy options. For SomaliREN to function effectively as a platform, clear service definitions are required, as well as agreed service levels, cost-sharing mechanisms that reflect recurrent operating costs, and an accountability model that balances central delivery with institutional responsibilities (e.g. local network readiness, account lifecycle management, and first-line support).

University consortia models are particularly useful when institutions have similar profiles or operate within the same geographical or governance context, as this makes collaboration easier to organise and govern. Consortia can facilitate

the joint procurement of bandwidth or licences, the shared hosting of selected services (e.g. a small group’s shared LMS), joint training and certification initiatives, and peer-learning networks centred on shared challenges. Compared with SomaliREN-wide services, consortia are lighter and faster to initiate, but quality and consistency can vary unless minimum standards and operating expectations are agreed upon from the outset.

Pooled procurement frameworks reinforce both the SomaliREN and consortium approaches by reducing price dispersion, limiting vendor fragmentation and embedding minimum technical standards in purchasing decisions. This is particularly important where institutions procure independently with inconsistent specifications and limited contractual leverage. Pooled procurement can be applied to connectivity service agreements, networking equipment and spares, backup solutions and selected software licences, while also standardising key safeguards such as service levels, reporting requirements, data protection clauses and exit/portability provisions. Over time, this shifts ad hoc acquisition towards more sustainable lifecycle planning.

EARDIP can act as a catalyst. It can be used to reduce the risks associated with early shared delivery by financing initial onboarding, the expansion of the shared platform, and the establishment of core operational capabilities, such as service management routines, reporting, and support boundaries. This creates a bridge to sustainable cost-sharing, where recurrent operating costs are progressively absorbed through predictable institutional contributions rather than remaining grant-dependent.

Three conditions are critical for the success of all shared delivery models. Firstly, shared services must be defined as operational products with clear ownership, service levels and support boundaries, rather than one-off installations. Secondly, cost sharing must explicitly account for ongoing operating costs; otherwise, services will deteriorate once the initial funding ends. Thirdly, adoption must be evidence-based: institutions require a minimum level of

readiness, particularly with regard to Package D routines, consistent account management, and access control, before they can be onboarded to shared identity and platform services. These conditions determine which institutions can adopt shared delivery immediately and which require staged readiness support first.

7.3.2 Market-facing partnerships

Such partnerships are essential for scaling higher education digital transformation, as many of the required capabilities – such as reliable connectivity, secure hosting and specialist systems implementation – lie within the private sector. Given the national profile (predominantly Tier 1–3), market engagement should be sequenced and evidence-gated, prioritising reliability and operational support before advanced platforms or integration. However, the assessment findings also suggest that market engagement must be structured to avoid common failure modes, such as vendor fragmentation, under-specified service expectations, solutions that exceed institutional operating capacity and unforeseen recurring costs. This subsection therefore outlines the areas in which private-sector partnerships are most valuable across the investment packages and the contractual and governance safeguards needed to protect sustainability, performance and data integrity.

Licensed operators (operators and ISPs) are central to Package A and indirectly to Packages B and C, as connectivity quality determines the usability of shared services and institutional platforms. Partnerships with ISPs should be designed around measurable service performance rather than nominal bandwidth. Priority areas include:

- » Improving reliability through clearer service levels, faster fault response and proactive monitoring, fault response and restoration target
- » Introducing redundancy where feasible, such as secondary links, failover arrangements or alternative routing
- » Tailoring bandwidth management to protect priority academic and administrative services, fair-use policies and traffic management transparency

For many institutions, the most significant improvement is not necessarily higher bandwidth, but rather more predictable uptime, clearer escalation pathways and pricing structures that reflect the realities of the education sector. Where SomaliREN or consortia models can aggregate demand, they can also strengthen bargaining power and enable more consistent service standards across institutions, mirroring how NRENs achieve higher education connectivity gains in peer systems.

Vendors and systems integrators are particularly important for Package C (institutional systems and integration), as deployment success depends on factors such as implementation quality, workflow design, data migration and support arrangements, rather than simply software selection. Market engagement should therefore prioritise the following:

- » Fit-for-purpose solutions that are aligned to institutional scale
- » Implementation approaches that incorporate change management, documentation and staff enablement
- » Realistic integration designs that institutions can sustain.

A recurring risk in this area is procuring “feature-rich” platforms that exceed operational capacity, resulting in low adoption rates and the creation of parallel manual workarounds. To mitigate this risk, contracts should require deliverables beyond installation, such as configured workflows, role-based access, data ownership definitions, training, administrator handover and a support model with clear response times. Where possible, institutions and the government should also encourage interoperability and portability to reduce lock-in and preserve future options. Contracts should include acceptance checks tied to functional processes (e.g., registration-to-results workflow) and verified administrator handover.

Cloud and managed service providers can support packages B and D by offering hosting, backup, email/collaboration, monitoring and baseline security services, which individual institutions may struggle to operate in-house. Managed services

can be particularly valuable where staffing levels are low, as they convert complex operational requirements into predictable service arrangements – provided that oversight is robust and responsibilities are clear. The key is to treat managed services as operational contracts with measurable performance rather than as outsourced “black boxes”. Where feasible, managed services should be delivered through shared frameworks (e.g., SomaliREN-managed offerings or framework contracts) to reduce duplication and improve oversight.” Institutions must still maintain core governance responsibilities, such as access management, account lifecycle discipline, data classification and first-line support coordination. Managed service models also require explicit planning for recurring costs, renewal decisions and exit pathways.

A small set of non-negotiable safeguards should be built into procurement and contract management across all market-facing partnerships. EARDIP can be used to de-risk early upgrades by financing initial onboarding, performance monitoring set-up, and contract standardisation—while requiring credible plans for recurrent cost absorption.

» **Service levels and performance reporting:** contracts should define uptime targets, fault response times, escalation routes and reporting obligations. Without performance visibility, institutions cannot manage service quality or value for money.

» **Data protection and security obligations:** providers should be required to meet minimum security control standards, clarify their data handling practices and support incident reporting and response.

» **Exit, portability and lock-in protections:** Contracts should include provisions for data export, transition support and the ability to change providers without incurring excessive penalties or losing institutional data.

» **Total cost of ownership transparency:** Pricing should

clearly detail recurring costs (e.g. bandwidth, hosting, licences, support), and institutions should avoid commitments that cannot be sustained beyond the initial project period.

» **Capacity transfer and documentation:** Where vendors implement systems, they should deliver documentation, an administrative handover and training, enabling institutions to operate and adapt solutions over time.

7.3.3 Government’s enabling role and coordination mechanisms

Rather than providing ICT services directly, the government’s most significant contribution to the digital transformation of higher education is to establish the conditions that enable coherent, sustainable and equitable investments and partnerships across the sector. The assessment highlights significant variations in institutional readiness and demonstrates that the fragmentation of standards, procurement and operating models reduces the impact of investment. In peer systems, these coordination functions are often institutionalised through NRENs, enabling pooled procurement, shared services and consistent standards on a large scale. SomaliREN could fulfil a similar role in Somalia. In this context, the government (through MoCT, MoECHE and relevant oversight bodies) should provide the policy, coordination and accountability architecture that aligns institutions, SomaliREN and market partners around common baselines and implementable pathways.

The government can define a set of minimum baselines and standards that anchor implementation across tiers without prescribing a single technology choice. These baselines could cover minimum connectivity and power protection for critical ICT nodes, minimum cybersecurity and backup controls, minimum identity and access management practices for institutional systems and minimum service

management routines (e.g. incident logging and maintenance discipline). Where feasible, these baselines should be linked to Tier 1–3 pathways (with Tier 4 acting as a reference point) to help institutions understand what is expected at each stage and how progress will be assessed.

Coordinate investments around shared platforms and collective delivery. The government is well positioned to convene institutions and partners to deliver services more efficiently and improve quality, particularly where SomaliREN can operate as a platform for shared services and collective connectivity. Coordination mechanisms may include sector technical working groups, shared roadmaps for platform services and agreed service adoption pathways by tier. The government can also help to ensure that shared services do not become an unfunded mandate by making recurrent operating costs, service ownership, and cost-sharing arrangements transparent and aligned with institutional realities. EARDIP provides a time-bound opportunity to finance the build-out of shared platforms and the early onboarding of institutions, while also establishing sustainable cost-sharing for ongoing operations.

Strengthen procurement frameworks and reduce fragmentation. A key enabling factor is shifting procurement away from ad hoc, institution-by-institution acquisition towards strategic arrangements that embed standards and safeguards. These can include framework contracts, pooled procurement mechanisms, and model SLAs for connectivity, hosting, and managed services. Standard safeguards, such as service levels and performance reporting, data protection clauses and portability/exit provisions, can be embedded in procurement guidance to protect institutions, even when procurement capacity is uneven. For systems implementations, contracts should also include acceptance checks tied to functional workflows, verified documentation, and handover procedures. Over time, these measures will improve value for money and reduce the risk of long-term vendor lock-in.

Align incentives and financing with

sustainability. The government can promote sustainability by ensuring that recurrent costs are recognised and planned for. This includes encouraging institutions to formalise ICT budgeting and lifecycle planning and linking support to minimum institutional commitments in a way that is realistic for institutions at different stages of development. For instance, access to certain shared services or capital upgrades could be contingent upon evidence of fundamental operational procedures and reliable cost coverage plans, coupled with supportive technical assistance to assist lower-tier institutions in meeting these requirements. This approach strengthens accountability while remaining sensitive to institutional readiness.

Establish accountability and a learning cycle. The government can support a credible, sector-wide improvement loop by making periodic self-assessment and reporting using the e-readiness framework mandatory. This framework should be based on a lean set of priority indicators that map to tier progression. This should function as a practical monitoring tool to inform investment prioritisation, technical assistance targeting, and programme adjustments, not as a burdensome compliance exercise. A clear reporting cadence combined with light-touch verification (including sample-based checks) can reduce “paper compliance” and strengthen evidence-based decision-making.

Clarify roles and avoid over-centralisation. Effective coordination requires clear boundaries. The government should avoid assuming day-to-day operational responsibility for institutional ICT, which lies with higher education institutions (HEIs) and service providers. Instead, the government should set direction, convene and coordinate, standardise safeguards and ensure enforceable accountability across the ecosystem. SomaliREN should provide shared services where appropriate; institutions should retain local operational responsibility; and private partners should deliver under clear SLAs. When responsibilities are clear and standards are enforceable, partnerships become more credible, investments become more coherent, and sector-

wide progress becomes measurable and sustainable.

7.4 Sustainability, Financing and Incentives

The assessment findings suggest that, for many institutions, the limiting factor is not the absence of technological options, but rather the difficulty of sustaining ICT services once initial investments have been made. Chapter 7 therefore treats sustainability as a design requirement, rather than a consideration that comes later in the process.

7.4.1 CapEx vs. OpEx sustainability logic

A sustainable digital transformation requires capital expenditure (CapEx) to be separated from operational expenditure (OpEx), with both being planned for as part of the total cost of ownership. CapEx usually involves one-off investments, such as campus network upgrades, power stabilisation equipment, servers, and initial system deployment. In contrast, OpEx covers the ongoing costs required to reliably operate and maintain these investments, including charges for bandwidth and connectivity, electricity and fuel, licences and subscriptions, hosting fees, maintenance and spare parts, cybersecurity services and staff time for support, monitoring and continuous improvement. The assessment indicates that many failures occur when institutions primarily treat ICT as a project-based CapEx activity while failing to budget formally for the OpEx required to keep services running, particularly where structural constraints make connectivity, security, and shared platforms recurring cost drivers.

This distinction has practical implications for sequencing and partnership design. Packages A and C tend to incur visible CapEx, but their value depends heavily on OpEx-funded routines under Package D (service management, maintenance, monitoring, documentation and staffing), as well as OpEx commitments for shared services under Package B (e.g. identity management, hosting, backup and baseline monitoring), where relevant. Shared services often shift costs from

irregular, institution-specific spending to more predictable subscription or service-fee models, which can improve sustainability — but only if institutions recognise and plan for the recurring obligation. Without OpEx being protected, institutions often experience predictable patterns: infrastructure degrades due to weak maintenance, systems adoption stalls due to limited support capacity, security controls lapse due to inconsistent patching and monitoring, and service quality declines as bandwidth and licensing renewals become irregular.

For this reason, financing and incentive mechanisms should be designed to make OpEx visible and manageable. This includes requiring institutions to identify recurrent cost drivers from the outset, linking investment support to minimum sustainability commitments (such as an ICT budget line, basic maintenance provisions and renewal planning) and favouring delivery models that reduce the OpEx burden through shared services and pooled procurement, where feasible. EARDIP can help to reduce the risks associated with the transition by financing the initial onboarding and platform build-out, while also establishing credible cost-sharing and budget recognition for ongoing operations. In short, CapEx creates assets, but OpEx sustains services—and readiness progress depends on treating both as integral components of institutional planning.

7.4.2 Financing and cost-sharing models

Given the wide variation in institutional starting points and the recurrent cost pressures identified in the assessment, financing models must achieve two things simultaneously:

- » Enable initial upgrades and capability building
- » Establish a credible pathway for sustaining OpEx over time.

No single model will suit all institutions or packages. Instead, a small set of flexible cost-sharing archetypes can be applied across tiers and typologies, provided that roles, cost items, and performance expectations are clearly defined. EARDIP should be treated as a catalytic

financing window that can mitigate the risks associated with early pooled arrangements and the development of shared services, especially where system-wide benefits depend on collective action through SomaliREN.

Model 1: Donor or project “kick-start” with institutional co-payment (graduated cost-sharing)

This model is well suited to Packages A and D (and selected elements of B and C) in Tier 1–2 institutions, where there are significant upfront constraints. External funding covers a time-bound share of CapEx and/or start-up OpEx, while institutions contribute a defined co-payment – financial or in-kind – scaled to capacity. This co-payment should increase over time, enabling institutions to progressively absorb recurring costs such as bandwidth, maintenance, and support. A key design requirement is that there are measurable institutional commitments (e.g. ICT budget recognition, staffing allocation and minimum operational routines) to demonstrate readiness to sustain services once external support declines. EARDIP can be used to finance early onboarding and stabilisation in this model, while facilitating a transition to predictable institutional OpEx.

Model 2: Government-enabled shared services subsidy (platform support)

This model focuses public support on services that generate efficiency gains across the system, particularly under Package B (shared identity, hosting, backup and baseline monitoring/security tooling) and certain elements of Package D (shared templates, training pathways, standards and operational coaching). Rather than subsidising each institution’s procurement individually, the government supports the shared platform function, which is often operated through SomaliREN or structured consortium arrangements, so that institutions can access higher-quality services at a lower unit cost. The support design should explicitly state what is covered (e.g. core platform operations and shared tooling) and what remains the institution’s responsibility (e.g. local network readiness and account lifecycle discipline). This model is most effective when paired

with adoption conditions, service-level transparency, and cost-sharing rules that protect quality over time.

Model 3: Pooled procurement and framework contracting (cost reduction through aggregation)

This model uses collective purchasing power to reduce unit costs and limit vendor fragmentation, particularly with regard to bandwidth, networking equipment and spares, backup solutions and software licensing. Savings can be redirected to critical operational expenditure needs. Pooled procurement can be led by SomaliREN, a university consortium or government-supported framework contracting. However, it requires standard specifications and consistent safeguards, including SLAs, reporting, portability/exit provisions, and data protection clauses. This model is particularly valuable where institutions lack individual procurement leverage and where price dispersion and inconsistent specifications undermine sustainability.

Model 4: Performance-linked financing (results-based support)

This ties financing, often for Packages B, C and D (and selectively E), to verified achievement of minimum controls and measurable service improvements. Access to subsidised shared services or system upgrade support, for example, can be dependent on evidence of backup/restore testing, functioning incident logging, minimum access control practices or formal OpEx budget recognition. This approach reduces “paper compliance” by requiring practical evidence before scaling support. It should be implemented alongside a small number of indicators and light-touch verification, in order to avoid placing a high compliance burden on lower-tier institutions.

Model 5: Managed service contracting with predictable OpEx (service-based financing)

Where institutional technical capacity is limited, managed services can convert complex operational tasks into service contracts with predictable, recurring costs relevant to Package B (hosting, backup, monitoring, and baseline security

tooling), as well as aspects of Package D.

This model is effective when there is strong enough governance to manage vendor performance, and when contracts include non-negotiable safeguards such as SLAs, performance reporting, data protection obligations, and exit/portability provisions. However, it should be avoided where institutions cannot sustain recurring payments or lack the necessary oversight capacity, as it can create brittle dependency and hidden long-term costs.

Applying models by package and tier

In practice, models are often combined. Tier 1–2 institutions usually require start-up financing with a graduated co-payment system, reinforced by pooled procurement savings and early operational discipline (Package D). Tier 3 institutions benefit from performance-linked support based on evidence and the adoption of shared services that reduce duplication while strengthening standards. Tier 4 can be considered an aspirational stage, involving selective, high-impact investments (e.g. resilience and security hardening), paired with incentives to contribute to shared delivery and peer learning.

The design principle remains consistent across all tiers: financing should make operational expenditure (OpEx) visible; shared services should be costed as operational products; and cost-sharing should reinforce institutional responsibility rather than substitute for it. The most effective arrangements clearly define:

- » Who pays for what (CapEx vs. OpEx);
- » The minimum institutional commitments required; and
- » How performance and sustainability will be monitored over time.

7.4.3 Institutional sustainability requirements

Regardless of their tier, delivery model or funding source, institutions require a sustained digital capability to fulfil a small set of non-negotiable commitments. These requirements are not intended

as punitive compliance measures, but as practical conditions that protect investments from predictable failure, such as service degradation, security incidents, stalled platforms and recurring reliance on external troubleshooting. They represent the minimum conditions for absorbing investment without creating technical debt or recurrent service failure. They also provide a clear basis for partners and the government to target support, differentiate between institutions based on their readiness to absorb investment and link financing to realistic sustainability expectations.

» Visible ICT budget recognition and recurrent cost coverage

Institutions should maintain a clearly identifiable mechanism for ICT financing — ideally a dedicated budget line or an equivalent traceable allocation — and explicitly account for recurrent costs such as bandwidth, licences/subscriptions, hosting fees, power/fuel, maintenance and spares. This should include an annual renewal plan for critical services, to avoid “stop–start” operations that undermine reliability and trust.

» Minimum operational staffing and role coverage

Institutions should appoint accountable ICT leaders and ensure minimum staffing levels for core functions (network/systems administration, user support, and baseline security practices), appropriate to their size. Where staffing is limited, institutions should at least define who is responsible for first-line support and escalation, and how external support is accessed and managed.

» Basic service management discipline

Institutions should implement a lightweight helpdesk or a structured log for incidents and requests that is actively used. They should also define escalation paths and maintain a routine for the preventive maintenance of critical infrastructure and systems. This is essential for reducing recurring faults, building institutional memory, and improving service reliability over time.

» Baseline for assets, configuration

and documentation

Institutions should maintain an up-to-date register of ICT assets and basic configuration documentation for critical infrastructure and systems. This should include a simple network diagram and an inventory of core platforms and licences. Without this baseline, institutions may experience avoidable downtime, inefficient procurement and heightened security risk.

» Minimum cybersecurity and access control practices

Institutions should implement security controls that are proportionate to their scope. These should include defined access roles for core systems, routine patching for servers and critical applications (with basic change records) and basic perimeter/endpoint protections. These controls should be backed by clear responsibility assignment and a minimum incident reporting pathway.

» Backup discipline and restore testing

Institutions should schedule regular backups of critical systems and datasets, ensuring they have at least one protected copy, and conduct regular restore tests with documented results to confirm usability. This requirement is fundamental to ensuring operational continuity and reducing the impact of common failures and cyber incidents.

» Governance and decision-making that translates into execution

Institutions should have a functional ICT prioritisation and oversight mechanism that links needs to plans, approves key decisions, and tracks implementation, however lightweight it may be. This includes clarity on system ownership (i.e. who is accountable for the SIS/LMS and other core platforms) and basic change control for major configurations and upgrades.

» Adoption readiness for shared services and partnerships

Institutions participating in shared services (e.g., SomaliREN platforms) or managed service contracts should

fulfil the following minimum adoption responsibilities: consistent account lifecycle management; local network readiness; first-line support coordination; and adherence to agreed service-level and security requirements. Although shared delivery reduces duplication, but it does not remove the need for institutional discipline. Participation should therefore be governed by clear onboarding requirements and service boundaries.

» Minimum data governance and responsible handling of institutional data

Institutions should identify sensitive datasets, clarify ownership and access rights, and establish straightforward rules for storage, retention and sharing. This is particularly important as institutions expand their digital systems and explore AI-enabled tools. Rules should also cover the use of third-party cloud platforms and AI services with institutional data, in order to prevent unmanaged risks to privacy, security and integrity.

Implications for financing and support

These non-negotiable principles provide a practical basis for aligning incentives and targeting support. For example, access to certain capital upgrades or subsidised shared services could depend on evidence that these minimum conditions are being met. Institutions that are not yet able to meet these conditions could initially be prioritised for targeted operational and governance support (Package D), alongside staged requirements that match their current capabilities. This approach reinforces sustainability while respecting different capacity constraints.

7.5 Implementation, accountability and the learning cycle

The recommendations and delivery options set out in this chapter require an implementation strategy to turn them into long-term results. This section outlines the coordination, accountability and learning mechanisms required to manage a staged programme across diverse institutions, align partners around shared baselines and standards,

and ensure that progress is evidence-based rather than compliance-driven. The focus is on lightweight yet functional governance arrangements, a clear separation of roles among key stakeholders, and a monitoring and feedback cycle that supports continuous improvement and periodic reassessment. Implementation should also support collective delivery mechanisms, such as shared services, pooled procurement and coordinated connectivity, so that system-wide bottlenecks can be addressed through aggregation rather than through fragmented, campus-by-campus upgrades. EARDIP can be used as a catalytic programme vehicle to support early onboarding, the development of a shared platform and readiness-gated scaling, while establishing sustainable cost-sharing and accountability over time.

7.5.1 Implementation architecture and governance

Effective implementation requires a robust coordination structure that can align investments and partnerships while operating within capacity constraints. The proposed architecture comprises three functional layers: strategic oversight, technical coordination, and delivery execution. These layers are supported by a lightweight programme management/secretariat function that maintains cadence, documentation, and follow-through. Clear reporting and decision pathways between the layers are essential to prevent fragmentation and enforce readiness gating.

- » **Strategic oversight (steering function):** This is a sector-level steering function led by MoCT, in coordination with MoECHE and relevant higher education oversight bodies. This layer provides overall direction, endorses minimum baselines and sequencing principles, approves annual priorities and resolves cross-institutional issues that cannot be handled at the technical level. This layer should focus on decisions that shape coherence (e.g. standards, investment prioritisation, accountability and sustainability expectations), rather than day-to-day operations.
- » **Technical Coordination (Implementation/Technical Working Group):** A multi-stakeholder technical working group coordinates the design and consistency of implementation across packages and institutions. Its responsibilities include translating priorities into technical standards, templates and guidance, supporting package sequencing and readiness gating, coordinating the adoption of shared services and pooled procurement mechanisms, and consolidating implementation lessons into updated tools and guidance. SomaliREN should play a central technical role, particularly in designing shared services, defining operational requirements and supporting interoperability and platform standards.
- » **Delivery execution (institutional delivery leads and partners):** Each participating institution appoints an implementation focal point, typically the ICT director or head of ICT, who is responsible for coordinating internal stakeholders, maintaining minimum evidence for progression and ensuring that operational routines are implemented alongside investments. Delivery partners (ISPs, vendors, and managed service providers) deliver contracted outputs under defined service levels and reporting requirements. Performance is managed through agreed oversight mechanisms.
- » **Programme management, reporting cadence and decision gates:** Implementation should operate on a simple cycle involving regular operational reporting from institutions and service providers (e.g. monthly), periodic coordination reviews (e.g. quarterly) and an annual planning and reprioritisation cycle using evidence to adjust sequencing and support. Progression to more complex packages should be dependent on a standard “minimum evidence bundle” (e.g. uptime tracking, functioning support routines, restore tests and basic access controls) rather than procurement readiness alone. A light secretariat/PMO function (which may be hosted or supported through programme arrangements) can maintain dashboards, documentation, escalation tracking and meeting cadence, allowing steering and technical groups to focus on decision-making and problem solving.

Table 39 summarises the allocation of roles and expectations of accountability across the government, SomaliREN, institutions and partners. It uses a RACI-lite structure to clarify who is responsible for leading, providing support and coordinating and overseeing the main implementation functions.

Table 39 : Implementation roles and accountability

Key: L = Lead/Accountable, S = Support/Implement, C = Consult/Coordinate,

I = Informed/Receive reporting

Implementation function	MoCT	MoECHE / NCHE	SomaliREN	HEIs	Partners (ISPs/ Vendors/MSPs)
Programme secretariat / PMO (cadence, dashboards, evidence packs, escalation tracking)	L	C	S	S	I
Set minimum baselines and standards (technical and service, adoption gates)	L	C	S	C	I
Prioritisation and annual planning (packages, cohorts, sequencing)	L	C	C	C	I
Technical coordination / TWG facilitation (standards guidance, sequencing support, lessons)	C	C	L	S	C
Shared services design and service catalogue (Package B)	C	I	L	C	S
Shared services operations (NOC/ service platform, monitoring, support escalation)	I	I	L	S (first-line/local readiness)	S (as contracted)
Institutional implementation leadership (internal coordination, adoption, change mgmt.)	I	I	C	L	S (as contracted)
Infrastructure delivery and service provisioning (Package A connectivity/ power/network)	I	I	C (aggregation/ standards)	C	L
Systems implementation and integration delivery (Package C)	I	I	C	L (ownership)	L (delivery)
Operations and service management practices (Package D)	I	I	C	L	S (tools/training as contracted)
Cybersecurity baseline controls and incident escalation pathways	L (policy/ coordination)	C	S	L (local controls)	S (managed controls)
Data governance and privacy practice (institutional level)	C	L (education sector policy)	C	L	I/S (where applicable)
Procurement frameworks / model contracts / SLA templates	L	C	C	S	I
Performance monitoring and reporting (service levels, uptime, delivery progress)	L (sector view)	C	L (shared services metrics)	L (institution metrics)	S (service reports)
Verification, learning, and periodic reassessment (tier movement, evidence checks)	L	C	C	C/S	I

7.5.2 Monitoring and evidence of progress

Monitoring should support implementation and learning rather than creating a compliance exercise that is overly burdensome. The objective is to track whether institutions are:

- » Stabilising services
- » Strengthening institutional controls and operational routines
- » Progressing along tier pathways in a credible and evidenced way.

Due to the uneven capacity for documentation across institutions, the monitoring approach should be streamlined, evidence-based and aligned with the tier and typology logic used throughout the assessment.

Use a lean monitoring framework.

Monitoring should focus on a small set of “signal indicators” that reflect service performance and institutional capability rather than attempting to reproduce the full set of diagnostic indicators used in the baseline assessment. Indicators should be selected to: (i) cover the main package areas (reliability, shared services, systems, operations and governance/risk controls); (ii) be measurable using simple evidence; and (iii) inform management decisions regarding sequencing, targeting technical assistance and triggering corrective actions.

Evidence rules and practical documentation.

Progress should be validated using practical evidence that institutions and service providers can generate as part of normal operations. Examples include uptime and outage logs for connectivity and core services, helpdesk/ticket logs or structured incident registers, backup schedules and restore test records, patch/update schedules for critical systems, asset registers and network diagrams, and short service performance reports from partners against agreed SLAs. Where evidence is missing, this should be explicitly acknowledged, distinguishing between capabilities that are absent and those that are present but not yet documented, so that support can be targeted appropriately.

Reporting cadence and accountability.

It is recommended that a simple cadence is adopted: lightweight monthly operational reporting at institution level (covering service continuity, incidents and key routine compliance, such as backups); consolidated quarterly reviews at programme level to interpret trends and adjust support; and an annual reassessment cycle to review tier movement, update priorities and adjust sequencing. Shared services operated by SomaliREN and market-facing providers should report against agreed service levels using standard templates. This enables comparability across institutions and prevents “invisible” service degradation.

Use monitoring to trigger decisions.

Monitoring outputs should inform implementation decisions directly, rather than being treated as standalone reporting. In practical terms, results should be used to:

- » Gate progression to more complex packages (e.g. Integration or ai pilots) until minimum controls are in place
- » Identify institutions requiring targeted operational support (package d), even when infrastructure investments are underway
- » Detect recurring faults and adjust maintenance or vendor performance management
- » Form peer-learning cohorts around common bottlenecks revealed by trend analysis.

Tier movement and learning. Annual reassessment should confirm whether institutions are progressing along tier pathways (Tier 1–3 as observed during the assessment) and provide insight into effective practices in Somali contexts. This cycle should be transparent and constructive, documenting progress and highlighting persistent constraints while refining sequencing and partnership models over time. Where possible, the reassessment process should be aligned with the self-assessment tool, enabling institutions to use it for internal management purposes while allowing for sector-level aggregation to inform planning and accountability.

7.5.3 Risk management and safeguards

Implementation risks in the digital transformation of higher education are often predictable. Investments may fail to be sustained due to weak recurrent financing; services may degrade without operational routines; security incidents may occur where controls lag behind system expansion; and fragmented procurement may create vendor lock-in and inconsistent standards. Therefore, risk management should be embedded into programme governance as a practical discipline, using clear safeguards in procurement and delivery, as well as evidence-based sequencing gates and routine monitoring to detect early warning signs and trigger corrective action.

These safeguards should be applied consistently across packages and delivery models. These include minimum service levels and performance reporting for connectivity and managed services; data protection and access control requirements for systems and platforms; portability and exit provisions to prevent lock-in; and operational sustainability conditions, such as budget recognition and maintenance routines. Risk controls should also recognise institutional diversity; lower-tier institutions require additional support to meet minimum safeguards, while higher-tier institutions require controls to prevent complacency and manage complexity, particularly for integration and AI-related pilots. Table 40 summarise the main implementation risks, early warning signs and safeguards to be incorporated into procurement, governance and delivery oversight.

Table 40: Implementation risk and safeguards summary

Risk area	Typical failure mode	Early warning signs	Safeguards / controls (practical)	Primary owner(s)
Sustainability (OpEx underfunding)	- Services degrade after initial investment - Renewals lapse - Maintenance deferred.	- Frequent downtime - Lapsed licenses/ bandwidth - Repeated “emergency” repairs.	- Require ICT OpEx identification + budget recognition - Phased co-pay models - Maintenance schedules - Renewals calendar - Pooled procurement for cost control - EARDIP bridging support for onboarding with a cost-sharing transition plan	- HEIs (Finance and ICT) - MoCT (incentives and conditions)
Operational capacity / execution gap	- Systems exist but are not reliably operated - Heavy dependence on ad hoc external fixes.	- No incident logs - Repeated faults - Undocumented changes - Staff overload.	- Package D initiated early - Minimum ITSM routines (logs/escalation) - Documentation baseline - Clear role coverage - Capacity transfer clauses in contracts.	- HEIs - SomaliREN (peer support/ templates) - Vendors (handover)
Connectivity service quality	Nominal bandwidth but poor uptime and slow fault resolution.	- Outage complaints - No SLA reports - Unresolved faults - Congestion at peak times.	- SLAs with uptime and fault restoration targets - Performance reporting and escalation pathways - Redundancy where feasible - Demand aggregation where possible.	- ISPs - HEIs - SomaliREN (aggregation and standards) - MoCT (frameworks)

Cybersecurity and data breach	- Expanded digital footprint without baseline controls - Incidents unmanaged.	- Unpatched systems - Shared accounts - Abnormal activity - Backups not verified (no restore tests)	- Minimum controls (patching, RBAC, firewall/endpoint) - Incident reporting pathway - Backup and restore testing - Periodic basic audits - Managed security services where feasible.	- HEIs - SomaliREN (shared tooling and guidance) - Vendors/MSPs
Vendor lock-in and poor portability	- Institutions cannot switch providers or extract data - Costs rise.	- Proprietary dependencies - Unclear data ownership - Punitive exit terms.	- Portability and exit clauses - Data export requirements - Documentation handover - Preference for open standards/interoperability - Framework contracts.	- MoCT (model clauses) - HEIs (procurement/contract management)
Fragmented procurement and inconsistent standards	- Diverse specifications - Incompatible systems - Higher long-term cost.	- Multiple overlapping platforms - Inconsistent configurations - High support burden.	- Minimum baselines and reference specs - Pooled procurement/frameworks - Technical review prior to purchase - Standard SLA templates.	- MoCT - SomaliREN (reference specs/technical review support) - HEIs
Uneven adoption / change resistance	- Low uptake of systems - Manual workarounds persist.	- Low usage metrics - Parallel paper processes - Complaints from users.	- Clear system ownership - Workflow redesign and training - Phased rollout - Usage monitoring - Leadership enforcement for priority processes.	- HEIs (Leadership, ICT and units) - Vendors (training and support)
Premature complexity and overreach	- Integration/AI pilots launched before foundations - Failures amplify risk.	"Pilot sprawl" - Integration failures - Data quality issues - Security gaps.	- Sequencing gates (evidence-based) - Limit pilots - Require readiness checks - Define success criteria and stop/scale decisions - Stage integration after minimum discipline.	- HEIs - SomaliREN (technical guidance/guardrails) - MoCT (gating expectations)
Coordination failure (multi-actor)	- Overlaps, gaps, slow decisions - Duplicated efforts.	- Conflicting initiatives - Unclear ownership - Stalled implementation.	- Clear governance layers and decision rights - RACI-lite roles - Regular coordination cadence - Escalation mechanism - Consolidated reporting - PMO/secretariat function (may be supported through EARDIP arrangements)	- MoCT/MoECHE - SomaliREN - HEIs

8 Conclusions and Way Forward

Somalia's higher education sector is at a pivotal point in its digital transformation. While the assessment reveals pockets of meaningful progress, particularly where institutions have maintained basic connectivity, deployed key systems or established functional ICT teams, the overall picture remains uneven and is constrained by foundational issues relating to reliability, institutionalisation and sustainability. Across much of the sector, digital capability can be described as being in the early stages of development: while core services may exist, they are often fragile due to unreliable power and networks, inconsistent operational routines, limited documentation, and recurrent financing gaps. These conditions do not negate progress but rather highlight the need to convert assets into dependable services and transition from ad hoc implementation to managed, sustainable delivery.

A realistic way forward can be achieved within a 12–18 month timeframe if actions are sequenced and targeted using the assessment's tier-and-typology logic (with institutions mainly observed across Tiers 1–3 and higher maturity treated as an aspirational reference). The most immediate and credible gains will come from stabilising foundational infrastructure and reliability where these remain binding constraints, strengthening operational capability and service management to reduce recurring faults and reliance on external troubleshooting, consolidating and integrating core institutional systems only where minimum controls and support capacity exist, and expanding collective approaches, especially shared services and pooled procurement through SomaliREN and complementary consortia arrangements, where these reduce duplication and improve quality. This pathway is not a single national rollout. It requires tier-aware planning

and targeting sensitive to the typology, as well as financing models that make recurrent costs visible and manageable.

Delays incur additional costs and risks. Inconsistent maintenance and renewals cause infrastructure and systems to deteriorate over time, increasing the cost of restoration and replacement in the long term. Fragmented procurement and unmanaged vendor relationships increase lock-in and lifecycle costs. Security and data risks increase as digital footprints grow without the necessary controls, making incidents that could disrupt academic delivery and damage trust more likely and more impactful. Most importantly, delays entrench inequality between institutions: those starting from stronger positions continue to advance, while others fall further behind, making catch-up harder and more expensive over time. For these reasons, rather than waiting for perfect conditions, the sector should implement minimum sector-wide actions, align investments and partnerships around shared standards and delivery models, and establish a learning cycle to support continuous improvement. EARDIP provides a time-bound opportunity to catalyse this shift by accelerating collective connectivity and shared platform delivery through SomaliREN, and by establishing sustainable cost-sharing and accountability for ongoing operations.

Appendix A Survey Instrument

Purpose and Scope

SomaliREN is conducting an institutional e-readiness assessment to evaluate the current state of ICT infrastructure, systems, governance, and capacity at Somali higher education institutions. The aim is to identify gaps and opportunities in order to prioritise areas of support for digital transformation in teaching, learning, research and administration.

This survey focuses on institutional-level readiness rather than the experiences of individual users. The findings will inform the strategic planning, capacity building and infrastructure investment efforts of SomaliREN and its partners.

The questionnaire takes approximately 30 minutes to complete. It can be completed in one sitting or returned to as needed (if using a digital form).

The information provided will be used solely for analytical purposes and to inform national planning. Any public reporting will anonymise individual institutional responses. Only aggregated data will be shared beyond SomaliREN.

If you have any questions or require assistance with the survey, please email the SomaliREN technical team at: info@somaliren.org or call +252 612697979.

Your participation is crucial in building a robust evidence base to advance ICT in Somali higher education. Thank you for your time and commitment to this national effort.

Section A. Informed Consent

1. Do you consent to participate in this institutional e-readiness assessment survey?
 - Yes/No
2. If you selected “No”, please briefly explain your reason (optional).
 - Open text

Section B. Institutional Profile

This section collects essential background information about the university to support benchmarking and contextual analysis. Please provide the most accurate information possible for the current or most recently completed academic year.

1. Name of institution?
2. Please provide website address.
3. Type of institution?
 - Public
 - Private
 - Public–Private Partnership (PPP)
 - Community-owned /

Foundation

- Other (please specify)
4. Primary ownership or governing authority?
 - Government
 - Community Owned
 - Foundation
 - Private entity
 - Mixed
 - Other (please specify)
 5. Name of person completing this survey?
 6. Official position/role in the institution?
 7. Email address?
 8. Phone number?
 9. How many campuses does your institution have? (including the main campus)
 10. Where is the main campus located?

11. How many students does your institution have (both fulltime and parttime, across all campuses, if applicable)?
12. How many staff does your institution have (both academic and administrative)?
13. Year of establishment?

Section C. ICT Infrastructure and Systems

This section collects information on the availability, quality and distribution of ICT infrastructure and digital systems throughout the institution. Responses should reflect the current or most recently completed academic year.

1. Is your institution currently connected to the internet?
 - Yes/No/Not sure
2. Which internet access technologies do you use at your institution?
 - GSM/4G modem
 - VSAT/Starlink (satellite)
 - Microwave radio
 - Fibre optic
 - ADSL/DSL
 - Other
3. What is the fastest internet speed that your institution can achieve or has contracted with any internet service provider?
 - Less than 2mbps
 - 2mbps to less than 5mbps
 - 5mbps to less than 10mbps
 - 10mbps to less 30mbps
 - 30mbps to less 100mbps
 - More than 100mbps
 - I don't know

4. How much in total bandwidth do all Internet service providers provide to your institution per month (across all campuses/all connections)?
5. How much in total cost do all Internet service providers charge your institution per month (across all campuses/all connections)?
6. Does your institution have internet usage monitoring tools?
7. On average, how many hours per week is the internet down or unavailable?
8. Does your institution have internet usage monitoring tools?
9. Does your institution have a network connecting buildings across the main campus?
 - Yes/No/I don't know
10. What is the main network backbone technology?
 - Fibre
 - Copper (CAT5/CAT6)
 - Wireless bridges
 - Mixed
 - I don't know
11. What percentage of academic/admin buildings are covered by the LAN?
12. Please estimate the length of fibre on campus in Km.
13. Does your institution have a Wi-Fi campus-wide network?
14. What percentage of the campus do you think is covered by the Wi-Fi network?
 - Less than 25%
 - 25-50%
 - 51-75%
 - Over 75%
 - I don't know

15. Are there dedicated computer labs for student use?

- Number of labs
- Total lab computers
- Library
- Offices/administration

16. Approximately, what proportion of this equipment (computers, laptops, projectors, laptops) is fully operational this year?

- Less than 25%
- 25-50%
- 51-75%
- Over 75%
- I don't know

17. In your institution, this academic year, how many of the devices below are provided by the institution for teaching and learning purposes?

- Laptops?
- Tablets?
- Projectors?
- Smart boards / interactive whiteboards

18. Do devices meet minimum requirements for current software/platforms?

- All/Most/Some/None

19. Primary source of electricity for ICT infrastructure?

- Electricity grid
- Generator
- Solar
- Other

20. Does your institution use any renewable or green energy sources to support ICT operations (in addition to the primary source)?

- Solar power
- Hybrid solar-grid systems
- Battery storage / UPS

charged via renewable energy

- Other renewable sources
- No renewable energy used

21. Frequency of power interruptions affecting ICT services?

- Daily/Weekly/Monthly/Rarely

22. Does the institution have backup power specifically for ICT systems (e.g. UPS, generator, solar)?

- Yes/No/I don't know

Section D. Human Resources and Institutional Capacity

This section collects information about your institution's ICT staffing levels, technical capabilities and support systems. Please respond based on the current or most recent academic year.

1. Does your institution have a formally established and dedicated ICT unit, department or team?

- Yes/No

2. To whom does the head of the ICT unit report?

- Vice-Chancellor/President/Rector/Principal/Director
- Deputy Vice-Chancellor (Admin/Finance)
- University Secretary / Registrar
- Other

3. Official designation/title of the head of the ICT function

4. How many ICT Technicians?

5. How many Systems Administrators?

6. How many Network Engineers?

7. How many ICT Managers or Directors?

8. Others (specify other roles and number)

9. Is there at least one staff member formally assigned responsibility for the following roles?

- User support/helpdesk
 - Learning platform administration
 - Cybersecurity
 - Web developer
 - Data management/reporting
 - None of the above
10. What proportion of ICT staff have formal ICT qualifications (degree or diploma)?
- All/Most/Some/None
11. Do any ICT staff hold professional certifications?
- Yes/No
12. List examples of professional qualifications (e.g. CCNA, Microsoft essentials)
13. Has your institution provided any ICT training or professional development for its ICT staff in the past 12 months?
- Yes/No
14. Does the institution allocate a training budget for ICT staff annually?
- Yes/No
15. Does your institution use any of the following systems to support ICT operations?
- Helpdesk or ticketing system for ICT issues
 - Network monitoring tools (e.g., for bandwidth or downtime)
 - Asset/inventory management system
 - None
16. How are ICT support requests from users currently handled?
- Through formal system/tickets
 - Informally (e.g., by email or phone)
 - No structured process in place
17. Does the ICT unit implement any preventive maintenance routines?
- Yes, written and scheduled
 - Yes, informal or ad hoc
 - No preventive maintenance
18. Are there written Standard Operating Procedures (SOPs) or manuals for managing ICT systems?
- Yes/No
19. Does the institution contract any ICT functions to third-party providers?
- Yes, multiple services
 - Yes, limited services only (e.g., cabling, internet)
 - No
20. What types of services are outsourced?
- LAN/Wi-Fi deployment
 - Server hosting
 - Network security
 - Helpdesk
 - Maintenance/repairs
 - Other
21. Has your ICT unit experienced high staff turnover in the past 2 years?
- Yes/No
22. Are there currently any vacant ICT positions not filled due to funding or recruitment issues?
- Yes/No
23. How many vacant positions have not been filled?
- Yes/No/I don't know
24. Does the institution have strategies in place to retain qualified ICT staff?
- Yes/No/I don't know
25. Has the institution integrated national or regional digital

education goals into its ICT plans?

- Yes/Partially/No/I don't know

26. Are mechanisms in place to monitor ICT performance and service delivery?

- Yes/No/I don't know

27. Has your institution conducted any user satisfaction surveys in the past 3 years?

- Yes/No/I don't know

28. Has your institution conducted any internal or external ICT audits or reviews in the past 3 years?

- Yes/No/I don't know

Section E. ICT Governance, Policy and Strategic Planning

1. Does your institution have an official ICT strategy or master plan??

- Yes/No

2. In what year was the strategy developed or last updated?

3. Is the strategy formally approved?

- Yes/No

4. How well is the ICT strategy aligned with the overall institutional strategic plan?

- Very aligned
- Somewhat aligned
- Not aligned
- I don't know

5. Is there a defined implementation roadmap with timelines?

- Yes/No

6. Which of the following policy documents exist at your institution? (Yes/No/Not sure)

- Acceptable Use Policy (AUP) for ICT
- Cybersecurity or Information Security Policy
- Data Protection or Privacy Policy

- Procurement Policy for ICT

- Bring Your Own Device (BYOD) or Mobile Device Policy

- Open Educational Resources or Digital Content Policy

- Social Media Use in Teaching and Learning

- Policy for Staff and Student Email Accounts

- ICT Asset Management Policy

- ICT Helpdesk / Service Management Policy

- ICT risk management policy or framework

- Backup and Disaster Recovery Policy

7. How often are ICT policies reviewed or updated?

- Every year
- 2-3 years
- No fixed schedule
- Never updated

8. Does your institution have an ICT Steering Committee or equivalent governance body?

- Yes/No

9. Who chairs the committee?

- Vice-Chancellor/President/Rector/Principal/Director
- Deputy Vice-Chancellor (Admin/Finance)
- University Secretary / Registrar
- Other

10. Which stakeholder groups are represented?

- Academic staff
- Administrative staff
- Students
- Other

11. How frequently does the committee meet?
 - Monthly
 - Quarterly
 - Annual
 - Irregularly
 - Never
12. Does the committee have decision-making authority over ICT budgets or policies?
 - Yes/No

Section F. Core Digital Systems Availability

1. Does your institution have any of the following? (select all that apply)

Used (Yes/No), Name of platform used, Hosting (Local/Cloud/Hybrid)

- Student Information System (SIS)?
 - e-Learning or Learning Management System (LMS)?
 - Digital Library Management System (DLMS)?
 - Digital repository for publications and electronic theses and dissertations?
 - Finance or ERP System?
 - Human Resources Information System?
 - Document Management System?
 - Video Conferencing (e.g., Zoom)?
 - Plagiarism Detection Software?
2. Are LMS and SIS integrated?
 - Yes/No
 3. Are Finance and HR systems integrated?
 - Yes/No

4. Are Finance and SIS integrated?
 - Yes/No
5. Are Library and SIS integrated?
 - Yes/No
6. What proportion of academic programmes currently use a Learning Management System (LMS)?
 - Less than 25%
 - 25-50%
 - 51-75%
 - Over 75%
 - I don't know
7. Which of the following functions are automated or digitised at your institution?
 - Course registration
 - Student records/transcripts
 - Online exams/assessments
 - Staff recruitment or payroll
 - I don't know
8. How do users access these systems?
9. Separate logins for each system
 - Single Sign-On (SSO) or unified dashboard
 - Teaching and Pedagogical Integration
10. Which of the following digital teaching practices are adopted at your institution?
 - Posting course materials online
 - Use of multimedia content in lessons
 - Online forums, quizzes, or feedback tools
 - Delivery of fully online or blended courses
 - Use of virtual labs or simulation software
 - Not sure

11. Are there institutional guidelines or incentives to support integration of ICT into pedagogy?
 - Yes/No
12. If yes, please describe
13. Are faculty supported with the following?
 - Instructional design or e-learning units
 - Pedagogical training on use of digital tools
 - Peer mentoring or communities of practice
 - Not sure
14. Are students supported through
 - Digital literacy programmes
 - Orientation sessions on institutional systems
 - Not sure
15. Are teaching spaces equipped with ICT tools?
 - Yes/No
16. Does your institution have any policy or guidelines promoting digital accessibility?
 - Yes/No/I don't know
17. Do any of your institution's digital platforms support the following accessibility features?
 - Screen reader compatibility
 - Font size or contrast adjustment
 - Offline access to materials
 - Captions or transcripts for video/audio content
 - Use of local languages or multilingual materials
 - Low-bandwidth modes or mobile-friendly versions
 - None of the above
 - I don't know
18. Has your institution ever assessed whether digital systems are usable by persons with disabilities?
 - Yes
 - No
 - Not applicable / No students or staff with known disabilities
 - I don't know
19. Is there staff or unit at the institution responsible for promoting digital accessibility or inclusion?
 - Yes - dedicated unit or focal person
 - Yes - embedded in another office
 - No
 - I don't know

Section G. Financial Sustainability

1. Does your institution have a dedicated budget line for ICT?
 - Yes/No/Not sure
2. What percentage of the institution's total annual budget is allocated to ICT?
 - Less than 2%
 - 2 - 5%
 - 6 - 10%
 - Over 10%
 - I don't know
3. What does the ICT budget cover? (connectivity, hardware, salaries, etc.)
 - Internet connectivity and bandwidth
 - Hardware purchase and upgrades
 - Software licences and subscriptions
 - System maintenance and repairs
 - ICT staff salaries and benefits

- ICT training and development
 - Outsourced ICT services
 - Other
4. Has the institution developed any core digital systems internally without donor or external funding?
- Yes/No
5. If the institution currently lacks a dedicated ICT budget line, does it have an estimated or preferred ICT budget requirement?
- Yes/No/Not sure
6. What are the main sources of funding for ICT activities?
- Institutional core budget
 - Donor or project-based funding
 - Student technology/service fees
 - Revenue-generating ICT services (e.g. printing, labs)
 - Government or agency subsidies
 - Research grants or projects
 - Other
7. Approximate percentage of ICT funding from student fees or service charges
8. Which of the following cost-efficiency or recovery strategies are used?
- Shared or centralised ICT procurement
 - Bandwidth optimisation (e.g. caching, bandwidth shaping)
 - Cost-sharing or subsidies through SomaliREN or other partners
 - Internal monitoring of ICT expenditure and cost-effectiveness
 - Charge for services like printing or lab use

- None of the above
9. Are there formal procurement or financial approval guidelines specific to ICT?
- Yes/No
10. Is long-term sustainability of ICT systems explicitly considered in strategic or financial planning?
- Yes/No
11. Describe any key strategies or practices your institution uses to ensure ICT sustainability
- 3. Section H. AI and Emerging Technologies**
1. Does the institution have an AI strategy or formal guidance on the use of AI?
- Yes/No/Not sure
2. Which areas does the AI strategy cover?
- Ethical use of AI
 - Use of AI in teaching and learning
 - Use of AI in research
 - AI in administrative decision-making
 - Data governance and privacy for AI systems
 - Staff and student training on AI
 - Risk management and responsible use of AI
 - Other
3. Does your institution currently use any AI tools or platforms?
- Yes/No/I don't know

4. In which areas are AI tools being used?
 - Teaching and learning
 - Research
 - Administration
 - Library services
 - Cybersecurity
 - Other
5. Has the institution provided any training or awareness activities on AI for staff or students?
 - Yes/No/I don't know
6. What computing resources suitable for AI or machine learning does your institution have access to?
 - GPU-enabled servers
 - High-performance computing (HPC)
 - Cloud-based AI services
 - Locally deployed AI tools
 - None
 - I don't know
- Operating systems and software regularly updated and patched
 - None of the above
4. How are user accounts and access managed?
 - Password policy in place
 - Role-based access control (RBAC)
 - Centralised user management (e.g., Active Directory)
 - Manual and ad hoc account management
 - I don't know
5. Do ICT staff receive training in cybersecurity or data protection?
 - Yes - at least one training session in the last 2 years
 - No
 - I don't know
6. Do you back up institutional data?
 - Yes - regularly
 - Occasionally
 - No formal backup
 - I don't know

Section I. System and Network Security

1. Is the institution aware of and compliant with cybersecurity/data protection standards?
 - Yes/No
2. Is responsibility for ICT security formally assigned to a unit or role?
 - Yes/No
3. Which security measures are implemented at your institution?
 - Perimeter firewalls or intrusion prevention systems
 - Internal network is segmented
 - Wi-Fi access secured
 - Antivirus/malware protection on servers and user devices
 - Access control systems for sensitive systems
7. Are data backups automated or manual?
 - Automated
 - Manual
 - Mixed
 - I don't know
8. What types of data are backed up?
 - Student and academic records
 - Financial data
 - Staff records
 - Learning management content
 - Other

9. Where are the backups stored?

- On-site storage
- Off-site or cloud storage
- External hard drives / USBs
- I don't know

10. Have you tested your disaster recovery or backup restoration process in the last 12 months?

- Yes/No/ I don't know

11. Do your server room(s) or ICT equipment rooms have the following?

- Access control (e.g., locked room, badge access)
- Backup power (UPS/ generator)
- Cooling/ventilation systems
- Fire detection/suppression system
- Equipment labelling and inventory system
- None of the above

12. Has the institution conducted a formal ICT risk assessment in the past 3 years?

- Yes/No/ I don't know

13. Have you experienced any of the following in the past 2 years?

- System downtime due to power or hardware failure
- An internet outage lasting more than 1 day
- Attempted or successful cyberattack (e.g., phishing or malware)
- Data loss or corruption
- Breach of student or staff data
- None

14. Does the institution have an incident response plan or protocol?

- Yes/In development/No/I don't know

Section J. Open-Ended Reflections

1. What are the top 2-3 digital transformation priorities your institution would like to pursue in the next 3-5 years (e.g. infrastructure, systems, skills, governance)?
2. Please share any key challenges, strengths, or contextual factors affecting your institution's digital journey that were not adequately captured in the previous sections.
3. Please indicate any specific areas where SomaliREN, the Ministry of Communications and Technology, Ministry of Education or other public institutions can support your digital transformation goals?
4. Has your institution implemented any innovative, low-cost, or locally adapted ICT solutions that could be shared as best practice with other institutions?
5. Please share any final comments or considerations that you feel are important for interpreting your institution's responses.

Appendix A Indicator Definitions

Domain 1 – Infrastructure and Connectivity

Purpose of the domain – Assess whether an institution has the foundational digital and power infrastructure required to support teaching, learning, research, and administration.

This domain answers: Does the institution have the basic physical and connectivity foundations to operate digitally – and does it manage them intentionally?

Indicator Code	Indicator Name	Capability Assessed	Source Variables	Scoring Logic	Notes
IC-1	Internet connectivity is available	Existence of basic institutional internet access. Does not assess bandwidth, reliability, or performance	internet_connected	Binary: 1 = Yes; 0 = No	Foundational prerequisite. Kept binary to preserve minimum requirement signal.
IC-2	Internet access technology robustness	Highest-capacity internet access technology available to the institution as a proxy for connection quality and scalability	internet_technologies_1 (GSM/4G), internet_technologies_2 (VSAT/Starlink), internet_technologies_3 (Microwave), internet_technologies_4 (Fibre)	Max-points model (choose highest available): GSM/4G=1; VSAT=1; Microwave=2; Fibre=3. Normalise: score = points/3	Uses technology type as a conservative proxy for institutional-grade connectivity potential. Does not assume realised speed or uptime.
IC-3	Depth and robustness of internal network infrastructure	Internal network distribution capability across campus	lan, wifi_presence, fibre_length	Component-weighted sum: “Wi-Fi present = 1; LAN present = 2; Fibre backbone present = 3 (only where fibre_length > 0). Total points 0–6. Normalise: score = points/6	Differentiates ad hoc Wi-Fi from structured LAN and backbone fibre. Avoids “any present = 1” saturation.
IC-4	Students have access to shared computing facilities	Institution-managed shared computing access for students	student_labs, lab_count, lab_computers, library_computers	0–2 points: 0 = no shared computing signals (student_labs==0 AND lab_computers==0/NA AND library_computers==0/NA). 1 = some shared provision (any of: student_labs==1 OR lab_computers>0 OR library_computers>0). 2 = broader provision (any of: lab_count>=2 OR lab_computers>=50 OR (student_labs==1 AND library_computers>0)). Normalise: score = points/2.	Thresholds are intentionally conservative and proxy-based; the indicator captures presence and breadth, not adequacy per student
IC-5	Infrastructure monitoring and visibility practices exist	Basic operational visibility for managing ICT services	internet_monitoring	Binary signal: 1 = monitoring in place; 0 = no monitoring; NA = missing	Kept simple because your dataset currently has a strong single monitoring signal. If you later add network monitoring/helpdesk tooling, you can expand to 0–1–2.
IC-6	Power supply supports digital operations	Continuity of power for ICT operations (availability + resilience)	primary_power, power_backup	0–2 points: 0 = no reliable power signal (primary power missing/none AND no backup). 1 = primary power available or backup present (captures off-grid/backup-only cases). 2 = primary power and backup (power_backup==1). Normalise: score = points/2.	Context-critical. This reflects continuity capability without assuming outage frequency. If you later trust power_interrupt_freq, you can use it only for narrative (baseline), not scoring.

Domain 2: Human Resources and ICT Organisation

Purpose of the domain – Assess whether the institution has basic human capacity, organisational structure, and operating arrangements to support ICT systems.

This domain answers: Is ICT responsibility institutionalised, staffed, and supported – even at a minimal level?

Indicator Code	Indicator Name	Capability Assessed	Source Variables	Scoring Logic (v1)	Notes
HR-1	ICT function is formally organised	Formal institutional recognition of ICT as an organisational function	has_ict_unit	1 = Yes/0 = No NA = Missing	Structural signal indicating the existence of a formally recognised ICT function. Does not assess authority, resourcing, or effectiveness.
HR-2	Dedicated ICT roles exist	Presence of at least one formally identified ICT staffing role	ict_technicians OR ict_sysadmins OR ict_network_engineers OR ict_managers	1 = Any role exists 0 = None NA = Missing	Indicates the presence of ICT staffing roles, not role differentiation, staffing depth, or adequacy relative to institutional size.
HR-3	ICT operational capacity is ensured through outsourcing	Use of outsourcing to support ICT operational functions	Any ict_services_outsourced_*	1 = Any outsourced service 0 = None NA = Missing	Outsourcing is treated as a compensatory operational arrangement and does not imply internal ICT capacity or sustainability
HR-4	ICT staff capacity development is supported	Presence of institutional support for ICT staff capacity development	ict_training OR ict_training_budget OR ict_staff_certified	1 = Any investment 0 = None NA = Missing	Captures the presence of training, certification, or budgetary support signals. Does not assess coverage, frequency, or effectiveness of capacity development

Domain 3: ICT Governance and Planning

Purpose of the domain – Assess the formalisation and coverage of ICT governance instruments rather than their effectiveness or enforcement. Scores reflect the presence, breadth, and documentation of governance arrangements, not implementation outcomes.

This domain answers: Is ICT guided by strategy, governance, and oversight – rather than ad-hoc decisions?

Indicator Code	Indicator Name	Capability Assessed	Source Variables	Scoring Logic (v1)	Notes
GP-1	ICT strategy exists	Existence of a formally articulated ICT strategy or master plan	has_ict_strategy	1 = Yes/0 = No NA = Missing	Indicates the presence of an ICT strategy document or equivalent planning instrument. Does not assess implementation status, quality, or currency of the strategy
GP-2	ICT strategy is formally approved	Formal institutional approval of the ICT strategy	strategy_approved	1 = Yes/0 = No NA = Missing	Approval signals institutional recognition but does not imply resourcing, implementation progress, or enforcement
GP-3	ICT governance structure exists	Presence of a formal ICT governance or oversight structure	has_ict_committee	1 = Yes/0 = No NA = Missing	Captures the existence of a committee or equivalent governance body. Does not assess composition, authority, frequency of meetings, or effectiveness of oversight
GP-4	Breadth of ICT policy framework	Existence and coverage of formal, institution-wide ICT-related policies	policy_1 ... policy_12 (institution-wide ICT policy areas)	Score = (No of ICT policy areas documented as "Yes") ÷ 12. Result normalised to a 0–1 scale. "No" = 0; NA = Missing/ Don't know	Captures the breadth of ICT policy coverage across core governance areas. Does not assess policy quality, enforcement, currency, or operationalisation

Domain 4: Digital Systems and Learning Technologies

Purpose of the domain – Assess whether the institution has core digital systems in place and in use, and whether learning technologies are institutionally enabled, even if unevenly adopted.

This domain answers: Are digital systems and learning technologies present and usable at an institutional level?

Indicator Code	Indicator Name	Capability Assessed	Source Variables	Scoring Logic (v1)	Notes
DS-1	Breadth of core administrative digital systems deployed at institutional level	Extent to which core institutional admin functions are supported by formal digital systems	sis_used, erp_used, hris_used, repo_used, dms_used	Score = (No. of core admin systems reported as “in use”) ÷ 5. Result normalised to a 0–1 scale. “No” = 0; NA = Missing /Don’t know	Captures the breadth of administrative system coverage. Does not assess system integration, level of usage, data quality, or effectiveness of institutional processes supported by these systems
DS-2	Breadth of institutional learning and knowledge platforms	Availability of formal digital platforms supporting teaching, learning, and knowledge access	lms_used, dlms_used	Score = (No. of learning or knowledge platforms reported as “in use”) ÷ 2. Result normalised to a 0–1 scale. “No” = 0; NA = Missing / Don’t know	Indicates the availability of structured learning and knowledge platforms. Does not assess programme-level adoption, pedagogical use, instructional design quality, or accessibility of learning content
DS-3	Accessibility is considered in digital systems	Baseline accessibility acknowledgement	Any platform_accessibility_* OR accessibility_assessed_* OR accessibility_staff_* OR has_accessibility_policy	1 = Any signal/0 = None NA = Missing	Non-punitive

Domain 5: Financial Sustainability

Purpose of the domain – Assess whether the financial building blocks for sustaining ICT systems are visible and institutionalised, rather than whether ICT funding levels are sufficient or affordable.

This domain answers: Is ICT financing recognised, planned for, and managed – even at a minimal level?

Indicator Code	Indicator Name	Capability Assessed	Source Variables	Scoring Logic (v1)	Notes
FS-1	ICT budget recognition and commitment	Formal recognition of ICT costs within institutional budgeting processes	ict_has_budget_line, estimated_budget	0.75 if ict_has_budget_line = Yes. 0.25 if ict_has_budget_line = No and estimated_budget = Yes. 0.0 if both are No. Don't know treated as missing (NA).	Measures recognition and structuring of ICT costs, not budget size or adequacy. Informal estimation is treated as partial commitment and deliberately capped
FS-2	Breadth of ICT funding sources	Diversity of funding sources supporting ICT expenditure	ict_funding_sources_* (select_multiple_funding_sources)	Let k = number of funding sources selected (out of 6). Score = 0.0 if k ≤ 1; 0.25 if k = 2; 0.50 if k = 3; 1.0 if k ≥ 4. Don't know treated as missing (NA).	Emphasises diversification rather than funding volume. Does not distinguish between source types in terms of quality or sustainability
FS-3	Financial governance and sustainability mechanisms for ICT	Presence of governance practices supporting planned and sustainable ICT financing	ict_sustainability_planning, ict_procurement_guidelines, ict_recovery_methods_*	Composite score: (a) ict_sustainability_planning = Yes; (b) ict_procurement_guidelines = Yes; (c) any ict_recovery_methods_* = Yes. Score = (Number of components present) ÷ 3. If only one component is known, cap score at 0.33. Don't know treated as missing (NA).	Distinguishes between isolated controls (e.g. procurement rules) and broader sustainability intent. Capping prevents single signals from driving tier advancement

Domain 6: Data Security and Risk Management

Purpose of the domain – Assess whether the institution has any awareness of data security risks and any basic measures in place to protect systems and data.

This domain answers: Is data security recognised as a risk, and are there any basic safeguards or responses in place?

Indicator Code	Indicator Name	Capability Assessed	Source Variables	Scoring Logic (v1)	Notes
DSR-1	Data security awareness and responsibility	Institutional ownership and accountability for ICT security	compliance_awareness, security_unit	1.0 if responsibility for ICT security is formally assigned (security_unit = Yes). 0.5 if awareness of cybersecurity or data protection standards is reported but no formal responsibility is assigned (compliance_awareness = Yes only). 0.0 if neither is present. Don't know treated as missing (NA).	Distinguishes informal awareness from formal accountability. Does not assess adequacy of staffing, authority, or enforcement.
DSR-2	Basic security and access controls	Presence of layered technical, physical, and access control measures to protect institutional systems and data	implemented_measures_*, physical_protections_*, user_account_mgmt	Define three components: (a) at least one technical security measure implemented (implemented_measures_*); (b) at least one physical protection in place (physical_protections_*); (c) structured access management practices reported (any user_account_mgmt other than manual/ad hoc only). Score = (# components present) ÷ 3. If only one component is known , cap score at 0.33 . Don't know treated as missing (NA).	Rewards layered security practices. Does not assess effectiveness or configuration quality of controls. A score of 1.0 reflects the presence of multiple categories of safeguards, not validation of their effectiveness or coverage
DSR-3	Data backup and recovery practices	Institutional preparedness to prevent and recover from data loss	data_backup, backup_type, tested_disaster_recovery	Define three components: (a) institutional data backups exist (data_backup = Yes); (b) backups are automated or mixed (backup_type ≠ Manual); (c) disaster recovery or backup restoration has been tested in the past 12 months (tested_disaster_recovery = Yes). Score = (# components present) ÷ 3. If only backups are reported without further detail, cap score at 0.33 . Don't know treated as missing (NA).	Distinguishes presence of backups from operational readiness. Does not assess backup scope, frequency, or storage architecture.
DSR-4	ICT risk recognition and incident management	Whether institutions recognise ICT risks and have mechanisms to manage security incidents	ict_risk_assessed, incident_response	Define two components: (a) formal ICT risk assessment conducted in past 3 years (ict_risk_assessed = Yes); (b) incident response plan or protocol exists (incident_response = Yes). Score = (# components present) ÷ 2. Don't know treated as missing (NA).	Separates risk recognition from response capacity. Does not assess incident history, response effectiveness, or recovery outcomes.

Appendix B Benchmark Sources

Somalia/SomaliREN/Somalia-facing regional context

- World Bank Blogs – “Keeping students connected in Somalia”: <https://blogs.worldbank.org/en/digital-development/keeping-students-connected-somalia>
- World Bank Blogs – “Improved internet access connects Somali students to each other and global knowledge”: <https://blogs.worldbank.org/en/digital-development/improved-internet-access-connects-somali-students-each-other-and-global-knowledge>
- AfricaConnect3 – “SomaliREN succeeds in implementing the international service of eduroam”: <https://africaconnect3.net/somaliren-succeeds-in-implementing-the-international-service-of-eduroam/>
- UbuntuNet Alliance – “SOMALIREN driving transformation through research and education networking innovation”: <https://ubuntunet.net/stories/somaliren-driving-transformation-through-research-and-education-networking-innovation/>
- Scribd – “Assessing ICT Readiness in Somali Higher Ed” (presentation): <https://www.scribd.com/presentation/589169559/ASSESSING-ICT-READINESS-OF-HIGHER-EDUCATION-IN-SOMALIA-CHALLENGES-AND-OPPORTUNITIES>

Regional/cross-country/continental

- World Bank – “Feasibility Study to Connect all African Higher Education Institutions to High-Speed Internet” (PDF): <https://documents1.worldbank.org/curated/en/320071626434508906/pdf/Feasibility-Study-to-Connect-all-African-Higher-Education-Institutions-to-High-Speed-Internet.pdf>
- Knowledge Consulting Ltd (KCL) – “Breaking the Final Connectivity Barriers for Higher Education Institutions in Africa” (PDF): <https://kcl.co.ug/wp-content/uploads/2023/01/Circulation-Version-Breaking-the-Final-Connectivity-Barriers-for-Higher-Education-Institutions-in-Africa.pdf>
- KENET eReadiness portal – “E-readiness Survey of East African Universities Report 2009” (PDF): <https://ereadiness.kenet.or.ke/sites/default/files/E-readiness%20Survey%20of%20East%20African%20Universities%20Report%202009.pdf>
- EPAA (Education Policy Analysis Archives) – “Challenges of implementing e-learning in African universities” (PDF): <https://epaa.asu.edu/index.php/epaa/article/download/8772/3538/42257>
- ERIC (fulltext) – “Status of E-Learning in Public Universities in Kenya”: <https://files.eric.ed.gov/fulltext/EJ1102715.pdf>
- ASU Education – “Embracing E-Learning in Public Universities in Ethiopia and Uganda” (file): https://education.asu.edu/sites/g/files/litvpz656/files/2023-12/12-22-2024_J2_Embracing_e-Learning_PWFormatted.pdf

Kenya – NREN/higher education ICT/governance/systems/security

- Kenya Education Network (KENET) – Main site: <https://www.kenet.or.ke/>
- KENET – Impact Report 2023 (PDF): https://www.kenet.or.ke/sites/default/files/kenet_impact_report_2023_0.pdf
- KENET – 2021 Annual Core Data Report Highlights (PDF): https://www.kenet.or.ke/sites/default/files/2021_annual_core_data_report_highlights.pdf
- KENET eReadiness portal – 2022/2023 Annual Core Data Survey Report (PDF): https://ereadiness.kenet.or.ke/sites/default/files/ctools/2022/Annual_Core_Data_Survey_Report_2022_2023.pdf
- KENET – ICT Directors Forum (Universities, Research Institutes and Teaching Hospitals): <https://www.kenet.or.ke/blog/kenet-kenet-holds-ict-directors-forum-universities-research-institutes-and-teaching-hospitals>
- KENET – “What services does KENET provide?": <https://www.kenet.or.ke/node/26>
- KENET – Connectivity bundled services: <https://www.kenet.or.ke/content/kenet-connectivity-bundled-services-0>
- KENET – Training portal/wiki: https://training.kenet.or.ke/index.php/Main_Page
- KENET – “Latest on KENET Capacity Building”: <https://www.kenet.or.ke/kenet-training>
- KENET – FAQs: <https://www.kenet.or.ke/content/frequently-asked-questions-faqs>
- KENET-CERT – Homepage: <https://cert.kenet.or.ke/>
- UbuntuNet Alliance – KENET (member stories/category): <https://ubuntunet.net/category/members/kenet/page/2/>
- UbuntuNet Alliance – “The Journey of The First Kenyan Identity Federation, RAFIKI”: <https://ubuntunet.net/members/the-journey-of-the-first-kenyan-identity-federation-rafiki/>
- Commission for University Education (CUE) – PDF (Scribd): <https://www.scribd.com/presentation/779658782/COMMISSION-FOR-UNIVERSITY-EDUCATION>
- Mama Ngina University College – “Transforming Learning, Research and Working Environments using ICT”: <https://mnu.ac.ke/transforming-learning-research-and-working-environments-using-ict/>
- AfricaConnect3 – “Remote Teaching transforms learning at St. Paul’s University”: <https://africaconnect3.net/remote-teaching-transforms-learning-at-st-pauls-university/>
- Kenya Times (media) – “KENET Recognizes Moi University...”: <https://thekenyatimes.com/latest-kenya-times-news/moi-university-ranked-third-in-offering-blended-degree-programs/>
- Studocu (secondary) – “Challenges of Implementing E-Learning in Kenyan Public Universities”: <https://www.studocu.com/row/document/kisii-university/curriculum-development/challenges-of-implementing-e-learning-in-universities/86221644>
- KENET – Strategic Plan (PDF): <https://www.kenet.or.ke/sites/default/files/kenetstrategicplan.pdf>
- Office of the Data Protection Commissioner (Kenya) – Guidance Note for the Education Sector (PDF): <https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-for-the-Education-Sector.pdf>

Uganda – NREN/higher education ICT/governance/financing/security

- Research and Education Network for Uganda (RENU) – Main site: <https://renu.ac.ug/>
- RENU – Services catalogue: <https://renu.ac.ug/services/>
- RENU – Infrastructure/organisation profile (PDF): https://uvcf.ac.ug/wp-content/uploads/2025/02/RENU-Infrastructure_compressed.pdf
- UbuntuNet Alliance – “RENU Identity Federation (RIF) Joins eduGAIN”: <https://ubuntunet.net/stories/renu-identity-federation-rif-joins-edugain/>
- NORDUnet – “RENU Identity federation joins eduGAIN”: <https://nordu.net/renu-identity-federation-joins-edugain/>
- RENU-CERT – Site: <https://cert.renu.ac.ug/>
- GÉANT CONNECT Online – “RENU makes connectivity accessible to all through metro eduroam”: <https://connect.geant.org/2022/08/16/renu-makes-connectivity-accessible-to-all-through-metro-eduroam>
- Uganda budget portal – Kabale University vote report (PDF): https://budget.finance.go.ug/sites/default/files/Sector%20Spending%20Agency%20Budgets%20and%20Performance/Kabale%20University_21.pdf
- Makerere University – ICT Strategic Plan 2020–2030 (PDF): <https://policies.mak.ac.ug/sites/default/files/policies/Makerere-University-ICT-Strategic-Plan-2020-2030.pdf>
- Makerere University ICT Strategic Plan 2020–2030 (Scribd copy): <https://www.scribd.com/document/727129296/Makerere-University-ICT-Strategic-Plan-2020-2030>
- Ndejje University – “Directorate for ICT Support Visits RENU for ICT Knowledge Exchange”: <https://ndejeuniversity.ac.ug/directorate-for-ict-support-visits-renu-for-ict-knowledge-exchange/>
- AKU (Aga Khan University) – “Policy Academic Quality Framework UG-005” (PDF): <https://www.aku.edu/admissions/Documents/policy-academic-quality-framework-ug-005.pdf>
- Digital Watch Observatory – “Ugandan National Cybersecurity Strategy 2022–2026”: <https://dig.watch/resource/ugandan-national-cybersecurity-strategy-2022-2026>
- TOJET (academic journal) – article v24i4/24415 (PDF): <https://tojet.net/articles/v24i4/24415.pdf>

Rwanda – NREN/higher education ICT/governance/systems/financing/security

- UbuntuNet Alliance – “RwEdNet Roars Back to Life”: <https://ubuntunet.net/stories/rwednet-roars-back-to-life/>
- UbuntuNet Alliance – RwEdNet category (member news): <https://ubuntunet.net/category/members/rwednet/>
- University of Rwanda – ICT Department page: <https://ur.ac.rw/?-ICT-Department->
- University of Rwanda – ICT Policy (PDF): <https://ur.ac.rw/documents/policies/ICT%20Policy.pdf>
- University of Rwanda – ICT Master Plan (Part 2) (PDF): <https://ur.ac.rw/documents/policies/ICT%20Master%20Plan%20-%20Part%202.pdf>
- University of Rwanda – UR online learning at a glance: <https://ur.ac.rw/?UR-online-learning-at-a-glance-what-you-need-to-know-about-the-platform>
- University of Rwanda – “UR gets “smart classroom” to facilitate e-learning”: <https://ur.ac.rw/?UR-gets-smart-classroom-to-facilitate-e-learning>
- UNILAK – Directorate of ICT: <https://site.unilak.ac.rw/directorate-of-ict/>
- Education Profiles – “Rwanda | Technology | Education Profiles”: <https://education-profiles.org/sub-saharan-africa/rwanda/~technology>
- Rwanda Ministry of Finance & Economic Planning (MINECOFIN) – ICT Sector Strategic Plan (2018–2024) (PDF): https://www.minecofin.gov.rw/fileadmin/user_upload/Minecofin/Announcements/ICT.pdf
- MINECOFIN – “Smart Education Project to Receive Frw 30 billion financing boost”: <https://www.minecofin.gov.rw/news-detail/smart-education-project-to-receive-frw-30-billion-financing-boost>
- Rwanda National Cyber Security Authority (NCSA) – Cyber documentation: <https://cyber.gov.rw/documentation/>
- NCSA – “Rwanda launches CyberHub to boost cybersecurity skills and innovation”: <https://cyber.gov.rw/updates/article/nca-launches-cyberhub-to-boost-cybersecurity-skills-and-innovation/>
- KT Press (media) – “University of Rwanda Bought Expensive Software...”: <https://www.ktpress.rw/2025/07/university-of-rwanda-bought-expensive-software-it-has-no-capacity-to-use-for-14-years/>

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>