Check for updates

RESEARCH ARTICLE

REVISED Building Digital Trust in East Africa: The Role of National ID and ICT Policy in Somalia's Digital Transformation

[version 2; peer review: 2 approved]

Mohamed Adam Isak[1], Abdulkadir Jeilani Mohamud[2]

[1]Department of Computer Science, Somali National University, Somali National AI Center, Mogadishu, Banaadir, Somalia
[2]Department of Computer Science, Somali National University, Mogadishu, Somalia

v2 **First published:** 30 Jun 2026, **15**:1029
https://doi.org/10.12688/f1000research.182539.1
Latest published: 10 Sep 2026, **15**:1029
https://doi.org/10.12688/f1000research.182539.2

Abstract

Trusted digital identities sit at the heart of any modern, inclusive financial system. This paper investigates Somalia's transition from a fragmented digital landscape to a secure, integrated ecosystem through the lens of a "Three Pillars" framework: Robust Digital Identity, Comprehensive ICT Policy, and Proactive Cybersecurity Safeguards. Utilizing a qualitative multi-method approach, the study triangulates fifteen semi-structured interviews with regulators, financial experts, and civil society against a rigorous analysis of foundational policies, including the Data Protection Act (2023) and the Cybersecurity Law (2026).

Results indicate that Somalia's digital identity ecosystem—comprising e-Aqoonsi, HUBIYE, and the Certificate Delivery System (CDS)—serves as a technical anchor for financial inclusion, significantly bolstered by a July 2025 Central Bank mandate requiring National IDs for all banking transactions. These tools are supported by legal scaffolding under the Data Protection Authority and proactive security guardrails provided by the Somalia Computer Incident Response Team (SOMCIRT).

However, comparative analysis reveals that while Somalia has achieved technical parity with East African Community (EAC) peers in biometric capabilities, it remains an outlier due to its reliance on foreign data hosting, which poses risks to national data sovereignty. To realize Somalia's Centennial Vision 2060, the study concludes that the nation must bridge implementation gaps in rural digital literacy and technical capacity while transitioning toward local data infrastructure. The paper proposes a strategic roadmap for regional harmonization and enhanced institutional coordination to sustain

Open Peer Review

Approval Status ✓ ✓

	1	2
version 2 (revision) 10 Sep 2026	✓ view	✓ view
version 1 30 Jun 2026	? view	

1. **Abeer F. Alkhwaldi**, Dakota State University, Madison, USA

2. **Maria de Fátima Pina**, ISCTE-University Institute of Lisbon (Ringgold ID: 56061), Sintra, Portugal
University of Coimbra, Coimbra, Portugal

Any reports and responses or comments on the article can be found at the end of the article.

public trust in the emerging digital economy.

Keywords
Digital Identity, ICT Policy, Cybersecurity, Somalia's Digital Transformation, E-government.

Corresponding author: Mohamed Adam Isak (mohamed.isak@snu.edu.so)

Author roles: Isak MA: Conceptualization, Data Curation, Formal Analysis, Investigation, Methodology, Project Administration, Resources, Software, Supervision, Writing – Original Draft Preparation, Writing – Review & Editing; **Mohamud AJ**: Methodology, Project Administration, Validation, Visualization, Writing – Original Draft Preparation, Writing – Review & Editing

Competing interests: No competing interests were disclosed.

Grant information: The author(s) declared that no grants were involved in supporting this work.

Copyright: © 2026 Isak MA and Mohamud AJ. This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

How to cite this article: Isak MA and Mohamud AJ. **Building Digital Trust in East Africa: The Role of National ID and ICT Policy in Somalia's Digital Transformation [version 2; peer review: 2 approved]** F1000Research 2026, **15**:1029 https://doi.org/10.12688/f1000research.182539.2

First published: 30 Jun 2026, **15**:1029 https://doi.org/10.12688/f1000research.182539.1

REVISED **Amendments from Version 1**

Initially, we strengthened the theoretical frame of the study by adding a new subsection in Literature Review, "Theoretical Basis of Digital Transformation". It situates the digital identity reforms of Somalia within established theories of digital transformation. It refers to Vial's (2019) work on value-creation change, Mergel, Edelmann and Haug's (2019) research on digital transformation in the public sector, Fountain's (2001) theory of technology enactment, Meijer and Bolívar's (2016) theory of governance networks, and Heeks' (2020) paradigm of ICT4D, as well as the literature on digital transformation in the financial sector (Alkhwaldi, 2025; Abu-AlSondos et al., 2024; Shehadeh et al., 2023). The conclusion included a paragraph pertinent to these views and linked them to the three-pillar framework of the study.

Second, we have added a paragraph in response to a request for initial evidence of use, outlining preliminary publicly available registration statistics for the e-Aqoonsi national ID program (over one million enrolments as of November 2025, citing independent sources), with the caveat that granular disaggregated data were not provided directly by NIRA and these numbers should be considered indicative rather than precise.

Third, for the relevant claims we removed a duplicate technology-news citation that duplicated data already available in the original sources, in favour of NIRA's own platform documentation.

Additional 10 references were included to support these improvements. The comparative nation table (Table 1) was reformed for better clarity. The initial study is saved including the results, information and deductions.

Any further responses from the reviewers can be found at the end of the article

Introduction

Across East Africa, the rapid growth of digital financial services is transforming how people save, transact, and access credit—especially among populations previously excluded from formal financial systems (World Bank, 2025). Mobile money platforms, agent banking, and digital wallets have become powerful tools for economic empowerment (East African Community Secretariat, 2021). Yet, behind this progress lies a critical concern: the issue of digital trust (OECD, 2020). Many East African countries still struggle with fragmented identity verification systems, inconsistent cybersecurity protections, and mismatched regulatory frameworks (World Bank, 2023). In Somalia, the situation is even more complex. Prolonged instability and limited infrastructure have slowed the development of a secure, inclusive digital identity ecosystem (Centre for Internet and Society, 2023), although the Data Protection Act (2023) and the newly established Data Protection Authority now provide a legal framework to enhance trust and privacy protections (Federal Republic of Somalia, 2017, 2019).

Recognizing this, both national and regional actors are working to reverse course. The East African Community (EAC), for instance, is pushing for broader digital integration through strategic initiatives like the World Bank-supported Eastern Africa Regional Digital Integration Project (EARDIP) (World Bank, 2025). These efforts highlight a critical understanding: for digital systems to succeed, they must not only be technologically sound, but also rooted in local realities, human rights principles, and user trust.

In Somalia, tangible progress is underway through the National ICT Policy & Strategy 2019–2024 (Federal Republic of Somalia, 2019), the National Communications Law 2017 (Federal Republic of Somalia, 2017), and the ICT Regulatory Transformational Strategy 2023–2027 (National Communications Authority, 2025). These documents collectively aim to expand affordable internet access, promote e-Government services, reinforce regulatory frameworks, introduce enforceable data protection measures under Law No. 005/2023, and establish secure digital ID systems. Prominent initiatives such as e-Aqoonsi, HUBIYE, and the Certificate Delivery System (CDS) illustrate this commitment (NIRA, 2024a, 2024b, 2024c).

Importantly, these digital reforms align with Somalia's Centennial Vision 2060, the nation's long-term strategy to become a stable, inclusive, and middle-income country by the time it reaches its 100th year of independence. Vision 2060 places digital transformation and institutional trust at the heart of economic development, emphasizing the role of ICT in service delivery, governance, and citizen empowerment. However, achieving these ambitions depends on addressing foundational issues—such as fragmented identity systems, weak cybersecurity infrastructure, and low public trust—which this paper seeks to explore.

This paper proposes that the construction of digital trust in Somalia is built upon three essential pillars: Robust Digital Identity, Comprehensive ICT Policy, and Proactive Cybersecurity Safeguards.

- Pillar 1: Digital Identity serves as the foundation, utilizing systems like e-Aqoonsi, HUBIYE, and the Certificate Delivery System (CDS) to authenticate users and reduce fraud.

- Pillar 2: ICT Policy provides the legal scaffolding, primarily through the Data Protection Act (2023), which ensures the lawful processing of personal information.

- Pillar 3: Cybersecurity acts as the security guardrail, operationalized by the Cybersecurity Law (2026) and the Somalia Computer Incident Response Team (SOMCIRT) to protect critical infrastructure.

This paper examines how these three pillars, when integrated and aligned with regional efforts, can contribute to building digital trust and enabling financial inclusion—not only in Somalia but throughout the East African region.

I. Literature Review

A. Theoretical Foundations of Digital Transformation

Before turning to sector-specific literature, it is useful to situate Somalia's experience within broader theoretical debates on digital transformation (DT). Vial (2019) conceptualizes DT as a process triggered by digital technologies that provokes significant changes to an organization's or a society's value-creation paths through evolving structures, processes, and stakeholder relationships — a framing that captures why Somalia's shift from fragmented, paper-based identity verification toward an integrated digital ecosystem (e-Aqoonsi, HUBIYE, CDS) constitutes DT in the fullest sense, rather than a narrow technology upgrade. In the public sector specifically, Mergel, Edelmann, and Haug (2019) show that DT is best understood as a cultural, organizational, and technological change grounded in strategy, echoing this study's finding that Somalia's three pillars must be institutionally — not merely technically — aligned to build trust.

The socio-technical and institutional dimensions of this transition are further illuminated by Fountain's (2001) technology enactment framework, which argues that the developmental outcomes of ICT are not determined by the technology itself but are "enacted" through the institutional arrangements, organizational routines, and bureaucratic capacities of the adopting state — a lens that helps explain why Somalia's technical parity with EAC peers in biometric capability has not yet translated into equivalent institutional coordination or rural uptake. Complementing this, Meijer and Bolívar (2016) emphasize that digital governance is inherently a multi-actor, network-based process requiring collaboration among public agencies, private telecom and financial operators, and civil society — consistent with this study's finding that Somalia's digital identity ecosystem depends on coordination across NIRA, the Central Bank, private banks, and telecom-based mobile money operators. Finally, Heeks (2020) situates such reforms within the broader "digital-for-development" (ICT4D 3.0) paradigm, which stresses that digital public infrastructure in fragile and low-resource states carries distinct risks around data governance, platform dependency, and datafication — directly relevant to this paper's concerns over foreign data hosting and national data sovereignty.

These theoretical perspectives also extend into the financial-sector literature relevant to Somalia's Sharia-compliant banking system. Alkhwaldi (2025) identifies digital trust, financial literacy, and perceived quality-of-life benefits as key antecedents of fintech adoption, reinforcing this study's central claim that trust — not merely technical availability — determines whether digital identity tools translate into financial inclusion. Abu-AlSondos et al. (2024) survey the opportunities and organizational challenges of DT across business sectors, including talent shortages, legacy-system constraints, and change-management barriers that parallel the institutional-capacity and coordination gaps identified among Somali regulators and financial institutions in this study. Most directly, Shehadeh et al. (2023) provide empirical evidence that DT improves operational efficiency and competitive advantage specifically within Islamic banks — a finding with direct bearing on Somalia's predominantly Sharia-compliant financial sector and its dependence on trusted digital identity for KYC and account-opening processes. Together, these studies extend the paper's Three Pillars framework beyond its policy and legal focus, grounding it in wider theoretical debates on socio-technical change, institutional capability, and digital government evolution.

B. Financial Inclusion and Digital Payments in the EAC

Mobile money platforms, notably Kenya's M-PESA, have significantly broadened financial access for the unbanked (Vodafone Group, 2025). In Somalia, local mobile payment services such as EVC Plus by Hormuud Telecom and E-Dahab by Dahabshiil also play a crucial role in daily financial transactions. These platforms are widely adopted across the country, enabling users to send and receive money, pay bills, top up airtime, and access small-scale digital finance. Their accessibility—even in remote areas—has made them essential tools for driving financial inclusion in fragile settings.

The transformative impact of mobile money on financial inclusion has been extensively documented in Kenya. Jack and Suri (2014) found that M-PESA reduced transaction costs, improved risk-sharing among households, and enhanced financial resilience, particularly among low-income populations. These findings demonstrate the broader potential of mobile money platforms to promote inclusive economic participation and provide valuable lessons for other East African countries, including Somalia.

However, despite this progress, regional interoperability and regulatory inconsistencies continue to hinder cross-border financial integration (East African Community Secretariat, 2024). The Eastern Africa Regional Digital Integration Project (EARDIP) aims to address these barriers by harmonizing payment systems and e-commerce regulations across the region (World Bank, 2025).

In Somalia, digital finance is underpinned by the National ICT Policy & Strategy 2019–2024, which prioritizes affordable ICT access and digital literacy as prerequisites for financial inclusion (Federal Republic of Somalia, 2019). Complementary reports, including the ICT Sector Investment Study (Somalia Investment Promotion Office, 2022) and the World Bank Digital Economy Report (World Bank, 2022), stress the importance of regulatory reform, public-private partnerships, and digital infrastructure investment to unlock inclusive financial services.

Launched in 2007, M-PESA remains the region's most successful fintech innovation. With more than 60 million users across eight countries—including Kenya, Tanzania, Ghana, and Ethiopia—M-PESA enables mobile-based transactions such as money transfers, bill payments, and credit access through a network of over 660,000 agents (Vodafone Group, 2025). Its success offers insights for replication and scaling across the Horn of Africa, particularly in fragile markets like Somalia.

C. National ID Systems as a Tool for Trust

Robust national ID systems are critical for secure identity verification and trusted access to public and private services (World Bank, 2019a, 2019b). Countries such as Rwanda and Uganda have implemented successful digital ID frameworks through platforms like IREMBO and NIRA, which enable biometric-based authentication for a range of services (Republic of Rwanda, 2015; Republic of Uganda, 2015).

Somalia's National Identification Number (NIN) initiative seeks to emulate and localize these models by linking digital IDs with financial services. The National ICT Policy & Strategy 2019–2024 underscores digital identity as central to e-Government and financial inclusion (Federal Republic of Somalia, 2019), while the National Communications Law 2017 (Federal Republic of Somalia, 2017) and the Somalia Data Protection Act 2023 provide a legal basis for consumer protection, data privacy, and lawful processing of personal information in ID-linked services.

A major regulatory shift occurred in July 2025, when the Central Bank of Somalia (CBS), in partnership with the National Identification and Registration Authority (NIRA), mandated that all individuals must present a government-issued National ID to open or renew bank accounts, effective 1 September 2025. This directive establishes a standardized identity verification framework across all financial institutions and closes long-standing gaps in digital trust and user authentication (Somali National News Agency [SONNA], 2025a).

D. Cybersecurity in Digital Finance

As digital financial ecosystems expand, exposure to cyber threats—including fraud, data breaches, and system disruptions—also increases (OECD, 2020). Weak cybersecurity frameworks can discourage user trust and limit the adoption of digital financial services. Regional initiatives such as the Eastern Africa Regional Digital Integration Project (EARDIP) emphasize the importance of strengthening cybersecurity and data governance across the EAC (Federal Republic of Somalia, 2017).

In Somalia, earlier assessments identified major gaps in cyber readiness, prompting reforms and incident response planning (Federal Government of Somalia, 2020). This has advanced with the Cybersecurity Law (2026), which establishes a national framework for protecting infrastructure, securing systems, and managing cyber incidents (National Communications Authority [NCA], 2026a). The law also defines institutional roles and response mechanisms.

Complementing this, Somalia has operationalized the Somalia Computer Incident Response Team (SOMCIRT) as the national center for detecting and responding to cyber threats (National Communications Authority [NCA], 2026b), marking a shift toward a more coordinated approach.

However, challenges remain, including limited technical capacity, shortage of skilled professionals, and weak institutional coordination. Addressing these gaps is essential to ensure secure digital financial systems and sustain public trust.

E. Gaps in Literature

Although digital ID systems and financial technologies have been widely studied, few academic works focus on the intersection of ID systems and cybersecurity in fragile contexts such as Somalia. Regional strategies like the EAC E-Commerce Framework and Somalia's e-Government Strategy Terms of Reference call for deeper research into public service digitization and citizen participation—areas still underrepresented in scholarly literature (OECD, 2020).

II. Conceptual Framework

The conceptual framework for this study posits that digital trust is not a standalone technological achievement but a multi-dimensional construct emerging from the convergence of three foundational pillars: Robust Digital Identity, Comprehensive ICT Policy, and Proactive Cybersecurity Safeguards. In the context of a fragile state like Somalia, these pillars provide the necessary technical, legal, and operational infrastructure required to move from a cash-based, informal economy to an inclusive digital financial ecosystem.

Pillar 1: Robust Digital Identity (The Foundation)

At the base of the framework is Digital Identity, which serves as the primary mechanism for establishing "who is who" in the digital realm. In Somalia, this is operationalized through the National Identification and Registration Authority (NIRA) and its ecosystem of platforms:

- e-Aqoonsi: Provides biometric-based authentication (facial recognition and fingerprints) to ensure unique identity and reduce fraud. The platform allows citizens to access services remotely, including bank accounts, SIM registration, and welfare programs (SONNA, 2025b; NIRA, 2024a).

- HUBIYE: Acts as a real-time verification gateway, allowing financial institutions and government agencies to validate identities against the national database. The platform supports user-consented data sharing and is designed for interoperability, fostering trust in cross-sectoral digital transactions (SONNA, 2025b; NIRA, 2024a).

- Certificate Delivery System (CDS): Ensures the authenticity of foundational documents, such as birth certificates, which are necessary for tiered Know-Your-Customer (KYC) processes. It incorporates features like QR codes and digital signatures to ensure document authenticity and reduce forgery risks, improving public sector transparency and service delivery (MoIFAR, 2023). The framework views these tools as the "anchor" for trust, particularly following the 2025 Central Bank mandate requiring a National ID for all banking transactions.

Pillar 2: Comprehensive ICT Policy (The Legal Scaffolding)

The second pillar provides the legal scaffolding necessary to protect user rights and regulate the behavior of digital actors. Without enforceable laws, technological tools like digital IDs can lead to privacy concerns or data misuse. This study focuses on:

- The Data Protection Act (2023): This law establishes the legal basis for the lawful processing of personal information and creates the Data Protection Authority to oversee compliance.

- National ICT Policy & Strategy 2019–2024: This framework prioritizes affordable access and digital literacy as prerequisites for trust.

- ICT Regulatory Transformational Strategy 2023–2027: This aligns domestic goals with regional standards, ensuring that Somalia's digital growth remains compatible with the broader East African Community (EAC).

Pillar 3: Proactive Cybersecurity Safeguards (The Security Guardrail)

The third pillar acts as the security guardrail, protecting the system from external threats and system disruptions that could otherwise erode public confidence. The framework identifies two critical components recently introduced in Somalia:

- Cybersecurity Law (2026): This provides the legal mandate for protecting critical national infrastructure and defines the institutional roles for managing cyber incidents.

- Somalia Computer Incident Response Team (SOMCIRT): This serves as the operational center for detecting, preventing, and responding to threats such as phishing and data breaches. By transitioning from a reactive to a proactive security stance, Somalia aims to mitigate the risks associated with foreign-hosted data systems and enhance national data sovereignty.

Digital trust emerges through the systematic integration of three pillars as shown in Figure 1: Digital Identity as a technical anchor, ICT Policy as legal scaffolding for data rights, and Cybersecurity as a protective guardrail. This convergence facilitates Somalia's transition to an inclusive digital financial ecosystem. Harmonizing these reforms with EAC standards and Vision 2060 enables expanded access to Sharia-compliant finance and remittances for marginalized groups. Thus, digital transformation establishes a trusted foundation for economic empowerment and national data sovereignty.

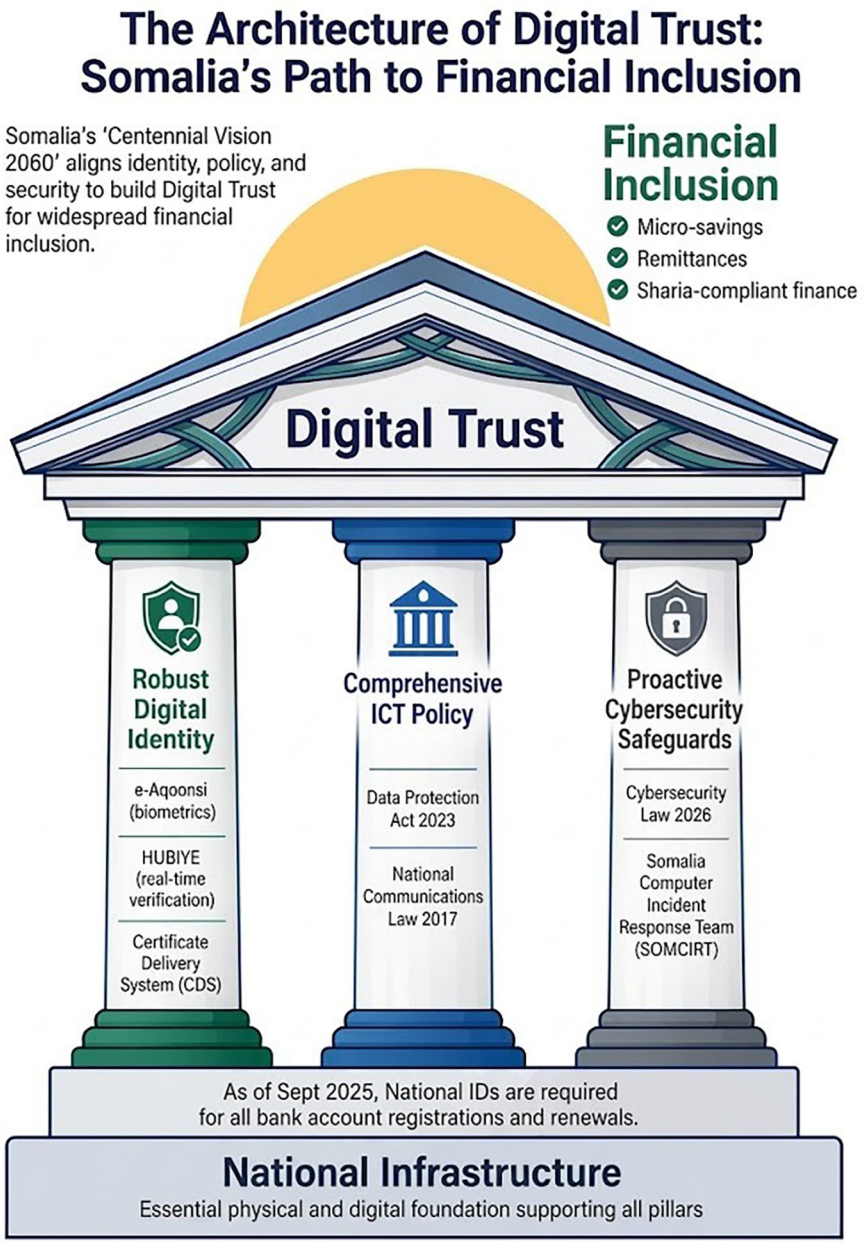


Figure 1. Temple of Trust model. *Note*: Conceptual framework developed by the author; visualization generated with assistance from Google Gemini (Google, 2025).

III. Data and Methodology

This study utilizes a qualitative, multi-method approach to capture the technical and social complexities of digital trust in Somalia. By combining primary insights from key stakeholders with a rigorous analysis of policy documents, the research provides a comprehensive view of how identity systems and regulations intersect to foster financial inclusion.

A. Research Design

The researchers followed a qualitative, multi-method approach, combining semi-structured interviews with document analysis, to capture firsthand insights and policy trends shaping digital trust in Somalia, within the broader East African context.

B. Data collection

- **Semi-Structured Interviews**

To capture nuanced perspectives on digital trust, fifteen key informants—including consultants, IT engineers, digital finance experts, bank staff, and civil society representatives—were interviewed between June 2025 and Jan 2026, via in-person and virtual formats using a conversational style with open-ended questions. To ensure the integrity and candor of the data, all participants provided informed consent regarding anonymity and confidentiality, with interviews held in neutral, private settings. Researchers' bias was mitigated through the systematic documentation of reflections in detailed field notes.

- **Policy review**

Primary interview data was triangulated with a rigorous review of foundational Somali legal and strategic frameworks. This included the National ICT Policy & Strategy 2019–2024, National Communications Law 2017, and ICT Regulatory Transformational Strategy 2023–2027. Critically, the review also examined the Data Protection Act (2023) and the Cybersecurity Law (2026) to evaluate the legal scaffolding of the digital ecosystem. These documents were analyzed alongside comparative features of other East African Community (EAC) national ID frameworks, as summarized in Table 1.

C. Ethical Considerations

This study was conducted in accordance with established ethical principles for research involving human participants, including voluntary participation, confidentiality, participant autonomy, and responsible data management. The research was designed as a minimal-risk qualitative study based on expert interviews addressing digital trust, cybersecurity, and financial inclusion within the Somali context.

In accordance with the institutional research guidelines applicable to the authors' affiliated institution, formal ethical approval was not required for this study, as it involved non-sensitive expert perspectives, did not include vulnerable populations, and posed no foreseeable risk to participants. Nonetheless, the study was conducted with strict attention to ethical responsibility, ensuring the protection, dignity, and rights of all participants throughout the research process.

Prior to participation, all respondents were fully informed about the objectives, scope, and academic purpose of the study, as well as the voluntary nature of their involvement. Participants were also informed that interviews would be audio-recorded solely for research and transcription purposes.

Informed verbal consent was obtained from all participants before each interview. Verbal consent was selected over written consent due to the specific nature of this research, which involved discussions of institutional, policy, and governance-related issues in Somalia. Many participants held professional positions in government or affiliated institutions, and requesting signed consent documents could create hesitation or perceived professional risk when expressing their views. Such formality could also affect the openness and depth of responses, which were critical for capturing authentic expert perspectives. Given that the study did not involve personal or sensitive individual data and relied on high-level professional insights, verbal consent was considered the most appropriate approach to ensure both ethical compliance and participant trust.

To ensure transparency and accountability, verbal consent was explicitly confirmed and documented at the beginning of each interview through audio recording and researchers' field notes. Participants provided consent for participation, audio recording, and the use of anonymized data for academic research and publication.

Table 1. Comparative Analysis of National Digital Identity Systems in Somalia and Selected East African Countries.

Country	Introduced	Biometrics	Smart Card	Mobile ID	Data Protection Law	Cybersecurity Law	Financial Integration	Data Hosting	Cross-Border Interoperability
Somalia	2022 (Pilot)	Yes	Yes	Yes	Yes	Yes	Full	Foreign	Planned
Kenya	2013	Yes	Yes	Yes	Yes	Yes	Full	Local	Yes
Uganda	2014	Yes	Yes	No	Yes	Yes	Full	Local	Yes
Rwanda	2015	Yes	Yes	Yes	Yes	Yes	Full	Local	Yes
Tanzania	2013	Yes	Yes	No	Yes	Yes	Full	Local	Yes
Burundi	2016	Yes	No	No	No	No	Partial	Local	Planned
South Sudan	2017 (Pilot)	Yes	No	No	No	No	Partial	Foreign	Planned
DRC	2018 (Pilot)	Yes	No	No	Draft	No	Partial	Local	Planned

Notes: Biometrics = fingerprint, facial recognition, or iris data used in identity verification. Mobile ID = availability of digital identity services through mobile applications or mobile-based credentials. Financial Integration = linkage with banking services, SIM card registration, digital payments, and government services. Local Hosting = data stored within national data centers; Foreign Hosting = data stored outside the country. Cross-Border Interoperability refers to the ability of national digital ID systems to integrate with regional identity frameworks such as the East African Community (EAC), COMESA, or ECCAS initiatives.
Source: Compiled by the authors from official government digital identity programs, national ICT policies, and regional digital governance reports (2025).

Interviews were conducted in secure and neutral settings, and no personally identifiable information was included in the analysis or reporting of findings. Audio recordings, transcripts, and field notes were securely stored and accessed only by the researchers for academic purposes. Participants were informed of their rights, including the right to decline participation, refuse to answer any question, or withdraw from the study at any time without consequence.

D. Data Analysis

Audio-recorded interviews were transcribed and systematically analyzed using NVivo software through a specialized two-phase coding process. First, thematic coding was applied to extract nuanced stakeholder perspectives on the "Three Pillars" of digital trust: identity authentication (e-Aqoonsi/HUBIYE), proactive cybersecurity (SOMCIRT), and public trust in Sharia-compliant financial systems. Concurrently, foundational policy documents—including the Data Protection Act (2023) and the Cybersecurity Law (2026)—underwent structural coding to map regulatory objectives against identified implementation gaps, specifically regarding data sovereignty and rural digital literacy. Finally, the synthesis of primary interview data and secondary policy analysis was triangulated with regional comparisons from the East African Community (EAC) to yield evidence-based, context-sensitive recommendations aligned with Somalia's Centennial Vision 2060.

IV. Results and Discussion

Synthesizing results from stakeholder interviews and comprehensive analysis of policy documents, this section evaluates Somalia's digital transition through the established three-pillar framework.

Pillar 1: Digital Identity as a Technical Anchor

National ID systems are widely regarded as essential infrastructure for secure digital transactions across the East African Community (EAC) (Gelb & Diofasi Metz, 2018; UNECA, 2019). In Somalia, the launch of e-Aqoonsi marked a significant turning point in accessibility; as noted by a Somali IT engineer in 2025, "The e-Aqoonsi app has enabled remote communities to obtain digital IDs without traveling to cities". While biometric authentication and real-time verification through HUBIYE have enhanced institutional trust, stakeholder interviews indicated that public awareness of these capabilities remains notably low in rural areas.

A critical regulatory milestone occurred in July 2025, when the Central Bank of Somalia mandated the use of a government-issued National ID for all banking transactions, effective September 2025,. This directive standardized identity verification across the financial sector and addressed long-standing authentication gaps. Finally, the Certificate Delivery System (CDS) streamlines the issuance of official documents, utilizing digital signatures and QR codes to reduce opportunities for corruption and exclusion (Gelb & Diofasi Metz, 2018; UNECA, 2019), (NIRA, 2024a). Together, these platforms establish the technical "anchor" necessary for expanding financial inclusion and building a resilient digital economy.

While comprehensive, disaggregated enrollment data were not made available to the researchers directly by NIRA, independent secondary reporting offers a useful proxy for the pace of adoption. As of November 2025, NIRA's Director-General reported that enrollment in the national ID programme had surpassed one million citizens, with more than two dozen public- and private-sector services — including banking and telecommunications — integrated for real-time authentication (Biometric Update, 2025). By January 2026, this figure represented approximately 7% of the government's stated target of 15 million registrations by 2029, with only around one-fifth of the estimated US$125 million implementation budget secured to date (Biometric Update, 2026). These figures should be read as indicative rather than precise, being drawn from public statements rather than NIRA's own disaggregated statistics; nonetheless, they corroborate this study's qualitative finding that rural and under-resourced populations remain substantially under-registered, and that sustained donor and government investment will be required to close this gap before Vision 2060.

Pillar 2: ICT Policy as Legal Scaffolding

The research highlights a critical shift from policy drafting to active legal enforcement, providing the "scaffolding" necessary to protect user rights.

The Data Protection Framework

The enactment of the Data Protection Act (Law No. 005/2023) and the establishment of a functional Data Protection Authority have created a legal basis for the lawful processing of personal information. This aligns Somalia with regional standards and addresses long-standing privacy concerns by introducing enforceable measures. Emphasizing the practical application of these protections, a NIRA staff member noted: "Consent features in the e-Aqoonsi app help build trust, but ongoing education is still needed".

Alignment with Vision 2060

These reforms are central to Somalia's Centennial Vision 2060, which prioritizes digital transformation as a means of governance and citizen empowerment. By placing institutional trust at the heart of economic development, the policy framework ensures that technology serves the broader goal of national stability. A Somali regulator underscored the importance of this human-centric approach, stating: "The success of e-Aqoonsi hinges not just on technology**,** but on whether citizens believe their data is safe and that the system works in their favor".

Regional Interoperability

As shown in Table 1, while Somalia has historically lagged behind East African Community (EAC) peers like Kenya and Rwanda, its recent legislative surge has significantly narrowed the regulatory gap,. However, challenges remain as cross-border interoperability and recognition of digital credentials currently remain in the "planned" phase rather than being fully active.

Pillar 3: Proactive Cybersecurity as a Guardrail

The transition from a "reactive" to a "proactive" security stance is marked by the introduction of institutional safeguards designed to protect critical infrastructure. As a cybersecurity expert reported during the research: "Without a proactive cybersecurity policy, we're always reacting to threats like phishing and SIM swaps".

Legislative and Operational Launch: The Cybersecurity Law (2026) provides the legal mandate for securing information systems, while the Somalia Computer Incident Response Team (SOMCIRT) serves as the operational center for detecting and responding to national cyber threats. This shift allows Somalia to complement regional efforts within the East African Community (EAC), where countries have made significant strides in establishing CERTs and consumer protections.

The Data Sovereignty Concern: A recurring theme in stakeholder interviews is the risk associated with foreign-hosted data systems, which leaves the digital ecosystem vulnerable to external data misuse. An advisor at the Ministry of Communications and Technology emphasized that: "Ongoing efforts toward data localization, including the development of local data hosting infrastructure, are expected to strengthen national cybersecurity by reducing reliance on foreign-hosted systems and improving control over sensitive information". Experts emphasized that until Somalia develops local data centers, its national sovereignty remains directly impacted by this technical reliance.

The findings suggest that digital trust in Somalia is not merely a byproduct of technology but is built through the alignment of these three pillars. As summarized in Table 1, Somalia has successfully matched its EAC peers in biometric and mobile ID capabilities. However, the study concludes that the final step toward a resilient digital economy requires moving from foreign hosting to local data sovereignty and ensuring that rural citizens believe their data is safe through ongoing education. As a Somali regulator emphasized: "The success of e-Aqoonsi hinges not just on technology, but on whether citizens believe their data is safe and that the system works in their favor". This trust is further reinforced by transparent "consent features" within platforms like e-Aqoonsi, which NIRA staff noted "help build trust, but ongoing education is still needed".

Comparing EAC National ID Systems

A comparative review indicates that Somalia has historically trailed its East African peers in data protection, cybersecurity regulations, and cross-border interoperability (see Table 1). While nations such as Kenya (NIRA, 2024b), Uganda (Republic of Rwanda, 2015), (Republic of Uganda, 2015), Rwanda (Republic of Rwanda, 2015), the Democratic Republic of Congo (DRC) (World Bank, 2019a), (World Bank, 2019b), and Tanzania (Somalia Investment Promotion Office, 2022), (Gelb & Clark, 2013) are actively piloting interoperable digital ID systems, Somalia's regulatory environment remained in a developmental drafting phase for a prolonged period.

However, the enactment of the Data Protection Act (Law No. 005/2023), the establishment of a functional Data Protection Authority, and the approval of the Cybersecurity Law (2026) have significantly reinforced the legal scaffolding and security guardrails necessary for institutional trust (NIRA, 2024a, 2024b, 2024c; SONNA, 2025a). This legislative progress establishes a robust foundation for personal data management, though Somalia remains the only regional actor identified as utilizing foreign data hosting rather than local infrastructure.

Implementation Gaps and Findings

Despite the technical and legislative milestones achieved through the three-pillar framework, research findings identify six critical implementation gaps that hinder the full realization of digital trust in Somalia.

- Infrastructure Inadequacy: Rural regions continue to face significant deficits in digital infrastructure, which restricts access to online identity services and limits the equitable distribution of financial tools.

- Digital Literacy Deficits: Awareness regarding digital rights and the functionality of platforms like HUBIYE remains low, particularly among marginalized populations. This lack of "digital citizenship" creates a barrier to effective system utilization.

- Biometric Enrollment Barriers: Technical challenges during the enrollment phase—ranging from hardware malfunctions to environmental factors—frequently affect the coverage, accuracy, and overall efficiency of the national ID database.

- Regulatory Enforcement Hurdles: While the Data Protection Act (2023) and Cybersecurity Law (2026) are now in force, an implementation gap persists. Institutional coordination between the Data Protection Authority and SOMCIRT is still evolving and requires sustained investment in human capacity.

- Data Sovereignty Risks: A recurring concern among stakeholders is the ongoing reliance on foreign-hosted data systems. This technical dependency raises significant national security concerns and remains a primary hurdle to achieving regional digital sovereignty.

- Data Transparency Gaps: Although e-Aqoonsi registrations are increasing, comprehensive empirical data regarding its direct impact on fraud reduction and financial inclusion remains unavailable.

The study concludes that while Somalia shows significant promise in digital identity transformation, its overall cybersecurity readiness and legal enforcement mechanisms still lag behind its EAC neighbors. As a Somali regulator underscored, the ultimate success of these initiatives hinges not just on technology, but on whether citizens believe their data is safe. Addressing these systemic gaps is essential to move from "digital potential" to a resilient, integrated, and inclusive digital economy.

V. Conclusion and Policy Implications

The findings of this study demonstrate that integrating digital identity systems with robust ICT and cybersecurity policies is both a technical and institutional imperative. Somalia's progress through the three-pillar framework—specifically the deployment of e-Aqoonsi, HUBIYE, and CDS—reflects meaningful advancement toward a secure digital ecosystem. However, the research indicates that without continued improvements in implementation capacity, digital literacy, and regional regulatory alignment, digital trust will remain limited. As a Somali regulator emphasized, the ultimate success of these initiatives hinges not just on the technology itself, but on whether "citizens believe their data is safe and that the system works in their favor". Read against the broader digital transformation literature, Somalia's trajectory illustrates that technical capability alone does not constitute transformation: as institutional and public-sector DT theory suggests (Mergel et al., 2019; Fountain, 2001), lasting change depends on how new digital infrastructure is enacted through existing bureaucratic capacity, multi-actor coordination, and citizen trust — the very dynamics this study's three-pillar framework was designed to capture.

The approval of the Cybersecurity Law (2026) and the establishment of SOMCIRT represent a critical milestone in transitioning the nation from a "reactive" to a "proactive" security posture. Together, these reforms provide the legal scaffolding and operational guardrails necessary for securing digital infrastructure and reinforcing public trust. Nevertheless, the long-term impact of these milestones depends on sustained investment in human capacity and institutional coordination.

Based on the analysis and insights gathered from regulators, financial institutions, and civil society, the following policy recommendations are proposed:

- Accelerate Regional Harmonization: Collaborate with EAC and continental bodies to align digital ID, data protection, and cybersecurity frameworks, leveraging initiatives such as the Eastern Africa Regional Digital Integration Project (EARDIP) to ensure cross-border interoperability (Federal Republic of Somalia, 2017), (East African Community Secretariat, 2022).

- Enforce National ID Mandates: Fully implement the Central Bank's directive to mandate National ID usage across all financial platforms—including mobile money and fintech services—to standardize identity verification and reduce fraud (Somali National News Agency [SONNA], 2025).

- Operationalize Legal Frameworks: Ensure the effective enforcement of the Data Protection Act (2023) and Cybersecurity Law (2026) through the full resourcing of the Data Protection Authority and its integration with SOMCIRT's incident response mechanisms (DataGuidance, 2023), (National Communications Authority [NCA], 2026a), (National Communications Authority [NCA], 2026b).

- Prioritize Rural Digital Literacy: Expand targeted literacy programs in underserved communities to bridge the "awareness gap" identified by stakeholders, ensuring that marginalized populations understand the consent features and protections available to them (National Communications Authority, 2025).

- Achieve Data Sovereignty: Invest in local data centers to transition from foreign-hosted systems to local hosting. This is a prerequisite for strengthening national cybersecurity and mitigating risks associated with external data misuse (Federal Government of Somalia, 2020).

- Strengthen Evidence-Based Policymaking: Establish monitoring and evaluation mechanisms for digital ID usage and public trust indicators. This should include tracking the impact of biometric enrollment on financial inclusion for rural women and other marginalized groups (National Communications Authority, 2025), (Republic of Uganda, 2015), (Federal Government of Somalia, 2023).

Ultimately, Somalia's experience demonstrates that digital trust is built not only through technological innovation, but through the alignment of legal, institutional, and operational frameworks that place the citizen at the center of the digital transformation.

Ethics Approval Statement

According to the institutional research guidelines of Somali National University, formal Institutional Review Board (IRB) approval was not required for this minimal-risk qualitative study involving voluntary expert interviews and non-sensitive professional perspectives. The study was conducted in accordance with internationally accepted ethical principles for research involving human participants, including voluntary participation, confidentiality, participant autonomy, and responsible data management.

Informed Consent Statement

Informed verbal consent was obtained from all participants prior to the interviews and audio recordings. Verbal consent was adopted due to contextual and professional considerations associated with discussions on institutional, policy, and governance-related issues within the Somali context, where written consent could affect participants' openness and willingness to share professional perspectives. Consent was documented through audio-recorded confirmation and researchers' field notes. No minors or vulnerable populations were involved in the study.

Data Availability

The data supporting the findings of this study are not publicly available due to confidentiality and participant privacy considerations. However, anonymized interview data may be made available by the corresponding author upon reasonable request for academic and research purposes. Requests for access to the data may be directed to:

Dr. Mohamed Adam Isak, Email: Mohamed.Isak@snu.edu.so

Access to the data is subject to ethical considerations and approval by the corresponding author to ensure participant confidentiality is maintained.

References

Abu-AlSondos A, Shehadeh M, Ajouz M, *et al.*: **The role of digital transformation in business: Opportunities, challenges and future directions.** *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Manama, Bahrain.* 2024; pp. 361–365.
Publisher Full Text

Alkhwaldi AF: **Digital transformation in financial industry: antecedents of fintech adoption, financial literacy and quality of life.** *Int. J. Law Manag.* 2025; **67**(6): 697–723.
Publisher Full Text

Biometric Update: **Somalia to integrate more govt services with national ID as issuance reaches 1M.** 2025, November 26.
Reference Source

Biometric Update: **Somalia requires $125M to fully implement national digital ID system.** 2026, January 12.
Reference Source

Centre for Internet and Society: **Data protection Africa: Policy tracker.** 2023.
Reference Source

DataGuidance: **Somalia data protection act (Law No. 005/2023).** 2023.
Reference Source

East African Community Secretariat: *EAC regional payment and settlement systems integration: Master plan 2021–2031.* Arusha, Tanzania: 2021.

East African Community Secretariat: *Treaty for the establishment of the East African Community (Revised edition).* Arusha, Tanzania: 2022.

East African Community Secretariat: **East African Community central banks urged to adapt and embrace technology to facilitate cross-border financial transactions.** 2024, July 23.
Reference Source

Federal Government of Somalia, Ministry of Finance: *Somalia national cybersecurity assessment report 2019–2020.* Mogadishu, Somalia: 2020.

Federal Government of Somalia, Ministry of Finance: *Terms of reference for national CERT establishment plan.* Mogadishu, Somalia: 2023.

Federal Republic of Somalia: *National communications law.* Mogadishu, Somalia: 2017.

Federal Republic of Somalia, Ministry of Post, Telecommunications and Technology: *National ICT policy & strategy 2019–2024.* Mogadishu, Somalia: 2019.

Fountain JE: *Building the Virtual State: Information Technology and Institutional Change.* Washington, DC: Brookings Institution Press; 2001.

Gelb A, Clark J: *Identification for development: The biometrics revolution (Working Paper 315).* Center for Global Development; 2013.

Gelb A, Diofasi Metz M: *Identification revolution: Can digital ID be harnessed for development?.* Center for Global Development; 2018.

Google: **Gemini [Large language model].** 2025.
Reference Source

Heeks R: **ICT4D 3.0? Part 1—The components of an emerging "digital-for-development" paradigm.** *The Electronic Journal of Information Systems in Developing Countries.* 2020; **86**(3): e12124.
Publisher Full Text

Jack W, Suri T: **Risk sharing and transaction costs: Evidence from Kenya's mobile money revolution.** *Am. Econ. Rev.* 2014; **104**(1): 183–223.
Publisher Full Text

Meijer A, Bolívar MPR: **Governing the smart city: a review of the literature on smart urban governance.** *Int. Rev. Adm. Sci.* 2016; **82**(2): 392–408.
Publisher Full Text

Mergel I, Edelmann N, Haug N: **Defining digital transformation: Results from expert interviews.** *Gov. Inf. Q.* 2019; **36**(4): 101385.
Publisher Full Text

Ministry of Interior, Federal Affairs and Reconciliation (MoIFAR): *Digital civil registry and certificate delivery system: Technical manual.* Mogadishu, Somalia: 2023.

National Communications Authority: *ICT regulatory transformational strategy 2023–2027.* Mogadishu, Somalia: 2025.

National Communications Authority (NCA): **Somalia's parliament approves the cybersecurity law.** 2026a, January 26.
Reference Source

National Communications Authority (NCA): **Somalia launches national cyber incident response center (SOMCIRT).** 2026b, March 7.
Reference Source

National Identification and Registration Authority (NIRA): *e-Aqoonsi mobile app user guide.* Mogadishu, Somalia: 2024a.
Reference Source

National Identification and Registration Authority (NIRA): *HUBIYE: Real-time digital ID verification system.* Mogadishu, Somalia: 2024b.
Reference Source

National Identification and Registration Authority (NIRA): *CDS platform overview.* Mogadishu, Somalia: 2024c.
Reference Source

OECD: *Digital security risk management for economic and social prosperity.* OECD Publishing; 2020.

Republic of Rwanda: *IREMBO digital platform overview.* Kigali, Rwanda: 2015.

Republic of Uganda: *National identification and registration authority (NIRA) annual report.* Kampala, Uganda: 2015.

Shehadeh M, Almajali D, Abu-AlSondos IA, *et al.*: **Digital transformation and its impact on operational efficiency and competitive advantage in Islamic banks.** *2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates.* 2023; pp. 1–6.
Publisher Full Text

Somali National News Agency (SONNA): **Somalia launches three key digital ID systems to enhance national identity infrastructure.** 2025a, May.
Reference Source

Somali National News Agency (SONNA): **National ID enforcement in Somalia: A strategic tool for the financial disruption of terrorist funds.** 2025b July 29.

Somalia Investment Promotion Office: *ICT sector investment study.* Mogadishu, Somalia: 2022.

United Nations Economic Commission for Africa (UNECA): **Digital ID and the data revolution: Opportunities and challenges for Africa.** 2019.

Vial G: **Understanding digital transformation: A review and a research agenda.** *J. Strat. Inf. Syst.* 2019; **28**(2): 118–144.
Publisher Full Text

Vodafone Group: **M-PESA: Africa's leading mobile money service.** 2025.
Reference Source

World Bank: **Democratic Republic of Congo – Identification for Development (ID4D) project (P167743).** 2019a.
Reference Source

World Bank: **Inclusive and trusted digital ID can unlock opportunities.** 2019b, August.
Reference Source

World Bank: *Somalia digital economy diagnostic report.* Washington, DC: 2022.
Publisher Full Text

World Bank: **Identification for Development (ID4D) global dataset.** 2023.
Reference Source

World Bank: *Eastern Africa Regional Digital Integration Project (EARDIP): Project appraisal document.* Washington, DC: 2025.

Open Peer Review

Current Peer Review Status: ✔ ✔

Version 2

Reviewer Report 21 October 2026

https://doi.org/10.5256/f1000research.209942.r526586

© **2026 de Fátima Pina M.** This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

✔ **Maria de Fátima Pina**
[1] School of Applied Digital Technologies, ISCTE-University Institute of Lisbon (Ringgold ID: 56061), Sintra, Portugal
[2] Institute of Systems and Robotics, University of Coimbra, Coimbra, Portugal

The article is well structured, with the introduction highlighting the relevance of the research and the objectives defined by three pillars, supported by literature. The methodology section is presented clearly, enabling the study to be replicated. The results are consistent with the objectives, and the research concludes with a summary that does not merely reiterate previous findings, whilst the authors also highlight the implications of the study.

In the meantime, I would like to offer a few brief comments which I believe might improve the research: firstly, I suggest that the authors remove the paragraphs from the abstract; secondly, only 15 interviews were conducted. Whilst this is acceptable for a qualitative study, it would be interesting to have a more detailed description of the sample's composition, for example, to know how many consultants and how many digital financial experts were included. Thirdly, the authors acknowledge that they do not have complete data on the reduction in fraud, the impact on financial inclusion, and the actual coverage of rural populations, which means that some conclusions are more forward-looking than empirically substantiated.

Further, the authors identify the objectives and create a simple conceptual framework within which they present qualitative evidence, concluding with recommendations. They responded clearly to the reviewers, refining the theory and linking it to the three-pillar model. The research is highly creative and relevant, adding value to existing theory. The research may be accepted for indexing, and if the authors deem it relevant, it could be slightly improved by incorporating the comments made.

Is the work clearly and accurately presented and does it cite the current literature?
Yes

Is the study design appropriate and is the work technically sound?

Yes

Are sufficient details of methods and analysis provided to allow replication by others?
Yes

If applicable, is the statistical analysis and its interpretation appropriate?
Yes

Are all the source data underlying the results available to ensure full reproducibility?
Yes

Are the conclusions drawn adequately supported by the results?
Yes

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: STEM areas

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.

Reviewer Report 22 September 2026

https://doi.org/10.5256/f1000research.209942.r520109

© 2026 Alkhwaldi A. This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abeer F. Alkhwaldi
Dakota State University, Madison, South Dakota, USA

The authors addressed all the required comments

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Digital Transformation

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard.

Version 1

Reviewer Report 02 September 2026

https://doi.org/10.5256/f1000research.201492.r515333

© **2026 Alkhwaldi A.** This is an open access peer review report distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

?

Abeer F. Alkhwaldi
Dakota State University, Madison, South Dakota, USA

This manuscript provides a timely and detailed empirical investigation into Somalia's evolving digital ecosystem. Using a qualitative multi-method approach combining 15 expert interviews with legal and strategic policy analyses the authors explore how digital identity platforms (e-Aqoonsi, HUBIYE, CDS), regulatory frameworks (Data Protection Act 2023), and cybersecurity infrastructure (Cybersecurity Law 2026, SOMCIRT) intersect to foster digital trust and financial inclusion. The conceptual "Three Pillars" framework effectively grounds the study, and the comparative assessment with East African Community (EAC) peers highlights key operational realities, such as data sovereignty challenges and rural digital literacy gaps.

Key Strengths

- **Contextual Significance:** Offers valuable insights into digital transformation in fragile state settings, an area often underrepresented in scholarly literature.
- **Methodological Triangulation:** Successfully balances primary stakeholder perspectives with a rigorous evaluation of key legislative texts.
- **Policy Relevance:** The strategic recommendations directly address core institutional barriers, such as local data hosting infrastructure and regional regulatory harmonization.

Areas for Improvement & Literature Integration:

While the paper is well-structured, expanding its grounding in broader academic literature would strengthen its analytical contribution:

- **Expand Conceptual Grounding on Digital Transformation:** The manuscript evaluates digital transformation primarily through a policy and legal lens. Incorporating broader scholarly literature on digital transformation dynamics specifically how socio-technical regimes, public-private actor networks, and institutional capabilities shape tech adoption in emerging economies would deepen the theoretical foundation.

Papers that are recommended to be cited:

- https://doi.org/10.1108/IJLMA-11-2023-0249
- doi: 10.1109/ICETSIS61505.2024.10459639
- doi: 10.1109/ICBATS57792.2023.10111266

- **Cite Core Digital Transformation Literature:** Consider engaging with established foundational and contemporary studies on digital transformation, enterprise digital maturity, and technology-driven public sector modernization. Contextualizing Somalia's trajectory within wider theoretical debates on digital government evolution and ICT-led socio-economic change will elevate the paper's academic contribution beyond its current policy focus.
- **Refine Empirical Impact:** If possible, include preliminary metrics or early usage estimates regarding e-Aqoonsi enrollment to complement the qualitative stakeholder insights.

Recommendation

Minor Revision. The paper offers strong empirical value and clear strategic roadmaps. Engaging more directly with broader academic literature on digital transformation will make this contribution even more impactful for researchers and policymakers alike.

References

1. Alkhwaldi A: Digital transformation in financial industry: antecedents of fintech adoption, financial literacy and quality of life. *International Journal of Law and Management*. 2025; **67** (6): 697-723 Publisher Full Text
2. A. Abu-AlSondos, M. Shehadeh, M. Ajouz, A. F. Alkhwaldi, M. Abdeldayem and S. H. Aldulaimi, "The Role of Digital Transformation in Business: Opportunities Challenges and Future Directions," 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS), Manama, Bahrain, 2024, pp. 361-365, doi: 10.1109/ICETSIS61505.2024.10459639.
3. M. Shehadeh, D. Almajali, I. A. Abu-AlSondos, A. F. Alkhwaldi and A. S. Al-Gasaymeh, "Digital Transformation and its Impact on Operational Efficiency and Competitive Advantage in Islamic Banks," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICBATS57792.2023.10111266.

Is the work clearly and accurately presented and does it cite the current literature?
Yes

Is the study design appropriate and is the work technically sound?
Yes

Are sufficient details of methods and analysis provided to allow replication by others?
Yes

If applicable, is the statistical analysis and its interpretation appropriate?
Yes

Are all the source data underlying the results available to ensure full reproducibility?
Yes

Are the conclusions drawn adequately supported by the results?
Yes

Competing Interests: No competing interests were disclosed.

Reviewer Expertise: Digital Transformation

I confirm that I have read this submission and believe that I have an appropriate level of expertise to confirm that it is of an acceptable scientific standard, however I have significant reservations, as outlined above.

Author Response 03 Sep 2026

Mohamed Adam Isak

Dear Reviewer,

Thanks for taking the time to read the manuscript and for your insightful remarks. We are delighted that the Three Pillars framework and the EAC comparative assessment were well received and we have amended the manuscript (Version 2) in response to your recommendations.

Broadening the theoretical underpinning of digital transformation.
We agree that the initial contribution focused primarily on digital transformation from the point of view of policy and law. We have added a new Literature Review section, entitled "Theoretical Basis of Digital Transformation", that situates Somalia's reforms in the broader socio-technical and institutional literature you identified, including all three of your recommended citations: Alkhwaldi (2025) on antecedents of fintech adoption and digital trust, Abu-AlSondos et al. (2024) on opportunities of digital transformation and organisational challenges, and Shehadeh et al. (2023) on the impact of digital transformation on operational efficiency in Islamic banks. The last two studies were especially pertinent to our consideration of KYC and account opening processes considering the mostly Sharia compliant financial sector in Somalia.

More generally mentioning core literature on digital transformation.
The new subchapter also addresses prior fundamental and present work on digital transformation dynamics: Vial (2019) on digital transformation as value-creation change Mergel, Edelmann and Haug (2019) on public-sector digital transformation Fountain (2001) on technology enactment theory Meijer and Bolívar (2016) on multi-actor digital governance networks Heeks (2020) on the ICT4D 3.0 "digital-for-development" paradigm. In the Conclusion, we have also included a final paragraph that directly connects these theoretical issues to our three-pillar framework, situating the paper's empirical findings in broader conversations about the growth of digital government and institutional competence.

Refining empirical impact with early usage estimates
We add a paragraph with preliminary enrolment data for e-Aqoonsi in the public domain (over one million registrations as at November 2025, independent reporting) and more recent budget and target figures announced in January 2026. These figures are not derived from NIRA's own disaggregated internal statistics, but from public statements, and hence we have expressly highlighted them as indicative rather than precise, but they do verify our qualitative conclusion of persistent rural under-registration.

We believe that these improvements further enrich the theoretical contribution of the manuscript, while maintaining its original empirical and policy focus, and thank you again for assisting us to sharpen the paper's engagement with the digital transformation literature.

Yours sincerely,
Mohamed Adam Isak (on behalf of the authors)

Competing Interests: No competing interests were disclosed.

The benefits of publishing with F1000Research:

- Your article is published within days, with no editorial bias
- You can publish traditional articles, null/negative results, case reports, data notes and more
- The peer review process is transparent and collaborative
- Your article is indexed in PubMed after passing peer review
- Dedicated customer support at every stage

For pre-submission enquiries, contact research@f1000.com

F1000Research