

Consultation on Ethiopia's E-Commerce Legal and Standards Frameworks

KISDI

2025

EUN JIN RYU
SOYOUNG SEO
JIHONG JOO

HANAH ZOO
GA YOUNG PARK





Consultation on Ethiopia's E-Commerce Legal and Standards Frameworks



This Report is published by KISDI as part of the “ICT Development Consultation Program: Delivering Co-Prosperity through ICT Development” sponsored by the Ministry of Science and ICT of the Republic of Korea.

KISDI Consulting Group

Korea Information Society Development Institute (KISDI)

Dr. Eun Jin RYU,

Fellow, Dept. of Global Digital Cooperation Research (Project Manager)

Ms. Soyoung SEO,

Associate Fellow, Dept. of Global Digital Cooperation Research (Project Officer)

Pusan National University

Prof. Jihong JOO,

Professor

Hallym University

Prof. Hanah ZOO,

Professor

Korea Advanced Institute of Science and Technology (KAIST)

Prof. Ga Young PARK,

Professor

Foreword

It is my great pleasure to introduce the report, “Consultation on Ethiopia's E-Commerce Legal and Standards Frameworks.” This report represents a significant milestone in Ethiopia's efforts to strengthen its digital economy and establish a trusted and enabling environment for e-commerce development.

As digital transformation accelerates globally, e-commerce has emerged as a critical driver of economic growth, market integration, and inclusive participation. In Ethiopia, while digital payments and connectivity have improved rapidly, the broader e-commerce ecosystem remains in an early stage of development, facing challenges related to regulatory fragmentation, limited trust mechanisms, and institutional coordination. Addressing these challenges requires a comprehensive and well-sequenced approach that integrates legal, technical, and institutional dimensions.

In response to this need, the Korea Information Society Development Institute (KISDI), in collaboration with the Ministry of Innovation and Technology (MinT) of Ethiopia, launched a two-year consultation program (2025–2026) under the support of the Ministry of Science and ICT (MSIT) of the Republic of Korea. The first year of the consultation focused on establishing foundational elements for Ethiopia's e-commerce ecosystem, with particular emphasis on (i) legal frameworks, (ii) transaction assurance standards, and (iii) alignment with regional digital trade frameworks, including the AfCFTA Digital Trade Protocol.

This report presents the key outputs of the first-year advisory. It includes policy recommendations for strengthening transaction assurance mechanisms, draft directives on intermediary liability and e-commerce licensing and registration, and analytical insights on Ethiopia's positioning within the evolving African digital trade landscape. These outputs are designed not as standalone solutions, but as part of a phased and adaptive process toward building a coherent, trusted, and sustainable e-commerce ecosystem.

Korea's experience in developing its ICT sector and digital economy has demonstrated the importance of strong institutional foundations, clear regulatory frameworks, and trust-building mechanisms. Through this consultation, KISDI aims to share relevant policy

insights and practical approaches while respecting Ethiopia's unique institutional context and development trajectory.

KISDI remains committed to supporting partner countries in achieving sustainable digital transformation and inclusive growth through knowledge sharing and policy cooperation. We hope that this report will serve as a valuable reference for policymakers, regulators, and stakeholders in Ethiopia and beyond.

Finally, we would like to express our sincere appreciation to the Ministry of Innovation and Technology (MinT) of Ethiopia for their close collaboration and leadership throughout this consultation. We also extend our gratitude to the Ministry of Science and ICT (MSIT) of Korea for their continuous support and guidance.

Sangkyu Rhee

President

Korea Information Society Development Institute

Table of Contents

Foreword	4
List of Figures	9
List of Tables	10
List of Abbreviations	12
Executive Summary	14
1. Introduction	17
1.1. Overview of the Consultation Program	17
1.2. Ethiopia's E-Commerce Landscape: Current Status and Challenges	20
1.2.1. Overview and Ecosystem Snapshot	20
1.2.2. Key Market Players and Platforms	21
1.2.3. Payment, Logistics, and Fulfilment Infrastructure	23
1.2.4. Market Trends and Usage Patterns	26
1.2.5. Digital Divide and Inclusion Challenges	28
1.2.6. Regulatory and Policy Environment	30
1.2.7. Practical Gaps and Emerging Opportunities	31
2. Standardization Framework for Transaction Assurance	34
2.1. Overview: Standards as a Policy tool for e-Commerce Trust Assurance	35
2.1.1. Trust Challenges in e-Commerce Transaction	35
2.1.2. Standards as a Policy Tool for e-Commerce Transaction	36
2.2. Consideration for Transaction Assurance: Key International Standards	39
2.2.1. ISO Technical Committee 321: Transaction Assurance in E-commerce	40
2.2.2. ISO 32111:2023 Principles and Framework for Transaction Assurance in E-commerce	41
2.2.3. ISO 32112:2025 Relevant Factors of Evaluation and Selection of Indicators	46
2.3. Case Studies: ROK e-Trust Mark Certification System (1999–2017)	64

2.4. e-Commerce Trust in Ethiopia and Recent Development	69
2.4.1. National e-Commerce Strategy (2024): focus on trust, standards, and platform quality	69
2.4.2. Policy environment and near-term priorities	71
2.4.3. Linking Current Developments to Transaction Assurance, Standards, and Trustmark Systems	72
2.5. Policy Recommendations for e-Commerce Transaction Assurance in Ethiopia	73
2.5.1. Mapping of Assurance elements to e-Transaction Phases	73
2.5.2. Mapping ISO 32111 Transaction Assurance Elements to Ethiopia's Legal and Institutional Framework	75
2.5.3. An Action Plan to Develop eTrust Mark Certification in Ethiopia	79
2.5.4. Suggested Timeline for Rollout	88
2.5.5. Addressing Implementation Challenges	89
 3. Legal Framework for E-Commerce : Draft Directives and Commentary	 90
3.1. Introduction: Rationale for Priority Legal Instruments	90
3.2. Intermediary Liability Directive (Draft)	93
3.3. E-Commerce Licensing and Registration Directive (Draft)	101
 4. Strategic Considerations for Ethiopia's E-Commerce and Regional Digital Trade Alignment	 108
4.1. Purpose and Scope of Strategic Considerations	108
4.2. Analytical Overview and Policy Coherence	110
4.2.1. Policy Orientation of Ethiopia's Request	110
4.2.2. Structural and Governance Constraints Affecting Ethiopia's Alignment with the AfCFTA Digital Trade Protocol	111

4.3. Stakeholder Landscape Overview for AfCFTA Digital Trade Implementation in Ethiopia	123
4.3.1. MinT's Legally Defined Mandate and Alignment with AfCFTA	123
4.3.2. MinT's Stakeholder Landscape Overview	125
4.4. Comparative Insights from Regional Experiences	132
4.5. Strategic Entry Points for Ecosystem Integration	142
4.6. Concluding Considerations	146
References	148
Annex	150

List of Figures

Figure 1-1	Ethiopian Adults with a Mobile Phone (%) 2024	29
Figure 2-1	ISO32111:2023 — Principles of Transaction Assurance	42
Figure 2-2	ISO32111:2023 — Activities during the Transaction Process	45
Figure 2-3	ISO32111:2023 — Assurance Elements and Participants	46
Figure 2-4	ISO32112:2025 Relevant Factors of Evaluation and Selection of Indicators	47
Figure 2-5	4 Factors and 18 Themes of Evaluation for e-commerce Transaction	48
Figure 2-6	Procedures to Select Appropriate Indicators	64
Figure 2-7	National e-Commerce Strategy: Goals related to e-Commerce Transaction Assurance	70
Figure 4-1	Fayda Platform API Specification Proposed Integration Model	143

List of Tables

Table 1-1	KISDI Consulting Group	19
Table 1-2	Interoperability Through ATM, POS, and P2P Transactions, 2020–2024	23
Table 1-3	Transaction Processed Through Digital Finance Services, 2020–2024 (numbers of transaction in millions and value in billions birr)	27
Table 2-1	Trust challenges in e-Commerce Transactions	35
Table 2-2	Policy Tools: Trust-building for e-Commerce Transaction	37
Table 2-3	Role of Standards in e-Commerce Trust Assurance	38
Table 2-4	ISO32111:2023—Participants and their Roles	44
Table 2-5	Example Indicators: Quality of e-commerce transaction platforms and sites	52
Table 2-6	Example Indicators: Quality of E-commerce Transaction Services	56
Table 2-7	Example Indicators: Local external environments for E-commerce transactions	60
Table 2-8	Example Indicators: Sustainability of E-commerce Transactions	62
Table 2-9	ROK eTrust Certification System: Legal Background	65
Table 2-10	ROK eTrust Certification System: Operating Agency	66
Table 2-11	eTrust Certification System Outline	66
Table 2-12	Evaluation Criteria	68
Table 2-13	Mapping the Assurance Elements: Pre-transaction Phases	73
Table 2-14	Mapping the Assurance Elements: In Transaction Phases	74
Table 2-15	Mapping the Assurance elements: Post-transaction Phases	75
Table 2-16	Mapping ISO 32111 Transaction Assurance Elements to Ethiopia's Legal and Institutional Framework	77
Table 2-17	eTrust Mark: Suggested Procedure for Pathway A	82
Table 2-18	eTrust Mark: Suggested Procedure for Pathway B	86
Table 4-1	Minimum Technical and Institutional Components for AfCFTA Digital Trade Readiness	121
Table 4-2	MinT Mandate based Digital Trade Mapping Table	124
Table 4-3	Inferred Operational Responsibility Structure (Based on the Draft Ethiopia National E-Commerce Strategy)	127

Table 4-4	Functional Overlaps and Gasp across Agencies (Draft Stage)	128
Table 4-5	MinT Actual Execution Gap (Based on the Digital Economy Strategy)	131
Table 4-6	Regional Benchmark Matrix for Digital-Trade Sequencing (Rwanda, Kenya, Ghana, South Africa, and Ethiopia)	136
Table 4-7	Ethiopia's Structural Challenges and Comparative Lessons from Kenya, Rwanda, and South Africa in the Transition from E-Transactions to Digital Trade	140
Table 4-8	Fayda's Current Capabilities vs. AfCFTA Digital Trade Trust Requirements (Overview)	145

List of Abbreviations

ADR	Alternative Dispute Resolution
AfCFTA	African Continental Free Trade Area
EAC	East African Community
ECOWAS	Economic Community of West African States
GCNet	Ghana Community Network
ICUMS	Integrated Customs Management System
ICT	Information and Communication Technology
INSA	Information Network Security Administration (Ethiopia)
ISO	International Organization for Standardization
KISDI	Korea Information Society Development Institute
LDC	Least Developed Country
MinT	Ministry of Innovation and Technology (Ethiopia)
MSIT	Ministry of Science and ICT (Republic of Korea)
M-PESA	Mobile Money Transfer Service
NBE	National Bank of Ethiopia
ODR	Online Dispute Resolution
PKI	Public Key Infrastructure
RISA	Rwanda Information Society Authority
UNCTAD	United Nations Conference on Trade and Development
WTO	World Trade Organization

Executive Summary

Ethiopia has identified e-commerce as a strategic priority in its Digital 2025 Strategy and requested Korea's technical and policy advisory support to strengthen its national digital trade ecosystem. In response, KISDI and the Ministry of Innovation and Technology (MinT) launched a two-year joint consultation program (2025–2026). The first year of the Ethiopia program focused on scoping, analysis, and foundational advisory work in three areas: standards for transaction assurance, and legal frameworks for e-commerce, and regulatory alignment with AfCFTA. The project began with an inception meeting in April and was followed by a July field study and consultation mission in Addis Ababa. A validation workshop attended by key Ethiopian stakeholders was conducted in December to review the analytic findings, receive feedback, and ensure local relevance and institutional feasibility.

Ethiopia's E-Commerce Landscape

E-commerce in Ethiopia is expanding but remains at an early and fragile stage of development. While digital payments have grown rapidly—supported by national payment infrastructure, mobile wallets, and emerging payment gateways—the broader e-commerce ecosystem continues to face persistent challenges. These include fragmented regulatory frameworks, limited transaction assurance mechanisms, weak dispute-resolution and enforcement structures, and low levels of consumer and merchant trust. Platform volatility remains high, with several well-known platforms exiting the market, while informal online commerce conducted through social media continues to dominate due to low entry barriers and limited formal alternatives.

Operational constraints in logistics and fulfilment—particularly last-mile delivery, addressing systems, and cross-border procedures—further limit scalability. In parallel, digital divides across gender, income, and urban–rural dimensions restrict inclusive participation, while institutional fragmentation weakens coordination among regulators, platforms, payment providers, and logistics actors. Together, these factors underscore that Ethiopia's primary challenge lies not in the absence of digital ambition, but in consolidating legal, technical, and institutional foundations into a coherent and trusted e-commerce framework.

Standards for Transaction Assurance

Against this backdrop, Chapter 2 presents the standards-related outputs of the first-year advisory, focusing on transaction assurance as a core trust-building mechanism for e-commerce. Drawing on Ethiopia's National E-Commerce Strategy, international practice, and relevant ISO standards, the report outlines a structured approach to developing a national transaction assurance framework.

A central proposal is the introduction of an Ethiopian eTrust Mark Certification to signal platform reliability, security, and compliance across the transaction lifecycle. To reflect Ethiopia's institutional context, the report explores two complementary pathways: a law-based voluntary certification model supported by explicit legal authority, and an ISO-aligned, standards-driven certification scheme developed through the national standards system. For each pathway, the report provides a phased implementation roadmap covering institutional roles, certification processes, auditor capacity, SME participation, and awareness-building, while identifying practical risks and mitigation measures.

Legal and Regulatory Frameworks

The legal advisory work in Year 1 focused on strengthening Ethiopia's e-commerce legal foundations through two complementary regulatory instruments. First, an Intermediary Liability Directive was developed to clarify platform responsibilities, liability allocation, notice-and-action procedures, and due diligence obligations—addressing a critical gap in platform governance and enforcement. Second, advisory inputs were provided for the development of an E-commerce Licensing and Registration Directive, aimed at establishing clear entry requirements, registration procedures, and baseline compliance obligations for e-commerce operators. Together, these instruments are designed to enhance legal certainty, support regulatory oversight, and facilitate the gradual formalization of Ethiopia's e-commerce market.

Strategic Context and Forward-Looking Considerations

Chapter 4 situates the legal and technical outputs within Ethiopia's broader e-commerce development trajectory and the evolving regional digital trade environment. Rather than presuming immediate implementation, the analysis highlights sequencing considerations, institutional linkages, and structural constraints that will shape future progress. It emphasizes the importance of moving beyond a narrow platform-centric view of e-commerce toward a comprehensive ecosystem approach encompassing payments, logistics, authentication, consumer protection, and data governance.

Conclusion

Taken together, the first-year consultation has established a grounded and coherent foundation for Ethiopia's e-commerce development by aligning market analysis with concrete legal and standards-based outputs. The report provides Ethiopia with practical tools, analytical clarity, and institutional reference points to support the gradual transition from framework design to implementation. These outcomes are intended to inform and strengthen the second year of the advisory program, which can build on this foundation through more targeted, operational, and capacity-oriented support.

Introduction

1.1. Overview of the Consultation Program

The Korea Information Society Development Institute (KISDI) has been implementing the ICT Development Consultation Program as part of an ODA project in the ICT sector with support from the Ministry of Science and ICT (MSIT) since 2002. Within this long-term cooperation framework, the current Consultation Program with Ethiopia was initiated as a two-year joint initiative between KISDI and the Ministry of Innovation and Technology (MinT), running from 2025 to 2026. This Program aims to support Ethiopia in designing the foundational legal and standardization frameworks required to develop a trusted, interoperable, and inclusive e-commerce ecosystem.

The Consultation Program officially began with an inception meeting held in April, during which both sides confirmed the shared intention to strengthen Ethiopia's e-commerce development in a way that is aligned with national priorities and institutionally feasible. The Korean team reaffirmed that all advisory support would be grounded in Ethiopia's policy goals, and that all policy decisions and next steps remain under MinT's leadership. Following the inception meeting, the KISDI consulting team visited Addis Ababa in July to share progress made in each advisory area. This trip also served as an opportunity to conduct on-site discussions and research, ensuring that our recommendations are grounded in Ethiopia's institutional context and practical needs. The July mission helped validate the initial direction of the project and further clarified Ethiopia's expectations for the Consultation Program.

To explain how the Year 1 advisory scope was finalized, it is important to revisit Ethiopia's initial proposal. During the Preliminary Feasibility Study conducted in February 2024, MinT expressed that “the general objective of developing ICT and digital economy standards, and directives, is to create a framework that promotes the effective and responsible use of technology in e-commerce and e-transaction services.” In line with

this objective, Ethiopia proposed eight advisory topics related to standardization policy and legal frameworks. Under standardization policy, the proposed topics included the development of information technology standards, the development of standards on electronic government services, and developing guidelines and procedures for data entry and verification of electronic messages. Under the legal framework domain, the proposed topics consisted of preparing communication of electronic messages directives, preparing limitations on the liabilities of intermediaries directives, preparing consumer protection directives in e-commerce, developing a federal electronic register of laws, and preparing directives on the management and maintenance of electronic messages.

Given the breadth and complexity of these eight topics, both sides agreed that narrowing the advisory scope would enable deeper, more actionable engagement within the two-year period. During the inception meeting in April, Ethiopia's priorities were reviewed again in light of the Digital 2025 Strategy, and the advisory focus was refined through discussions with MinT. Taking into account the topics initially proposed by Ethiopia, as well as their alignment with national policy direction, the scope was gradually streamlined with a clear emphasis on e-commerce.

As a result of the scoping process, the advisory project was structured around three themes for the first year. The first is legal frameworks related to e-commerce, including issues such as intermediary liability. For the legal frameworks, the first-year advisory focused on the preparation of draft directives addressing intermediary liability and e-commerce licensing and registration, which were identified as foundational regulatory priorities. The second theme concerns standardization frameworks, with a focus on transaction assurance in e-commerce. The third theme relates to policy coordination, particularly the alignment between Ethiopia's e-commerce strategy and regional digital trade frameworks under AfCFTA. While this policy coordination theme complements the preparation of legal and standards instruments, it was included to support their interpretation and future application within Ethiopia's evolving digital trade context. These themes were selected to provide practical and tailored recommendations that support Ethiopia's strategic priorities and ongoing efforts under the Digital 2025 Strategy.

Reflecting this structure, Chapter 2 presents the technical standards-related outputs of the first-year consultation, focusing on transaction assurance frameworks for e-commerce. Chapter 3 introduces the draft legal directives developed under the legal framework theme, including the Intermediary Liability Directive and the E-Commerce Licensing and Registration Directive. The detailed commentaries accompanying these directives are provided in a separate deliverables document prepared for consultation purposes. Chapter 4 situates these legal and technical outputs within a broader analytical and strategic context, examining Ethiopia's e-commerce development trajectory and its alignment with regional digital trade frameworks under the AfCFTA.

Throughout this process, the Korean advisory team maintained a clear understanding

of Ethiopia's policy priorities in the digital domain. The team carefully reviewed the Digital 2025 Strategy and expressed full support for the national emphasis on building digital trust, enhancing interoperability, and ensuring inclusive digital services. The advisory approach adopted for this project is designed to align with these goals and to help translate them into practical and sustainable legal, technical, and institutional solutions.

In December, a validation workshop was organized with the participation of key stakeholders from MinT and related institutions. During this workshop, the KISDI consulting team presented the analytic findings and draft advisory outputs, and received practical feedback directly from Ethiopia's policymakers, technical experts, and practitioners. This session provided an important opportunity to validate the relevance of the recommendations, to reflect stakeholder experiences into the advisory content, and to strengthen the collaborative nature of the project moving into the next phase.

The collaborative efforts undertaken throughout the year reflect the shared ambition of MinT and KISDI to structure the first year of the project around foundational, high-impact areas that can strengthen Ethiopia's e-commerce ecosystem and establish a strong basis for further development.

Table 1-1 KISDI Consulting Group

Organization	Participant	Position	Remarks
KISDI (Korea Information Society Development Institute)	Dr. Eun Jin RYU	Fellow	Project Manager (PM)
	Ms. Soyoung SEO	Associate Fellow	Project Officer
Pusan National University	Prof. Jihong JOO	Professor	Consultant (Legal framework)
Hallym University	Prof. Hanah ZOO	Professor	Consultant (Standards framework)
KAIST (Korea Advanced Institute of Science and Technology)	Prof. Ga Young PARK	Professor	Consultant (Digital Trade)

1.2. Ethiopia's E-Commerce Landscape: Current Status and Challenges¹

1.2.1. Overview and Ecosystem Snapshot

E-commerce in Ethiopia is emerging as a multi-layered ecosystem rather than a single digital platform. It encompasses a broad value chain that includes online marketplaces, digital payment systems, logistics and fulfilment services, data and trust infrastructure, and a wide range of sellers and consumers operating across formal and informal channels. The effective functioning of this ecosystem depends not only on the availability of digital platforms, but also on the coordination and interoperability of these underlying components.

From a development perspective, e-commerce holds significant potential for Ethiopia. It can expand market access beyond major urban centers, connect producers and consumers across geographic distances, and lower entry barriers for micro, small, and medium-sized enterprises (MSMEs). Digital channels also offer new opportunities for women entrepreneurs and youth, particularly where traditional labor market participation has been constrained by social norms, caregiving responsibilities, or limited access to physical marketplaces. In this sense, e-commerce is increasingly viewed as an instrument for inclusive growth within Ethiopia's broader digital transformation agenda.

At the continental level, e-commerce has also gained strategic importance through the African Continental Free Trade Agreement (AfCFTA), which seeks to promote cross-border digital trade, regulatory cooperation, and market integration across Africa. Ethiopia, as a signatory to the AfCFTA, has expressed a clear intention to participate in and benefit from these regional digital trade dynamics. The inclusion of e-commerce as a pillar in the Digital Ethiopia 2025 and 2030 strategies further reflects the government's recognition of its economic and developmental significance.

At the same time, Ethiopia's e-commerce ecosystem remains at an early and uneven stage of development. Structural challenges persist across multiple layers of the value chain. These include fragmented and payment-centric regulatory approaches, weak logistics and fulfilment capacity—particularly beyond major urban areas—limited interoperability among digital payment systems, and gaps in consumer trust, dispute resolution, and enforcement mechanisms. Market development efforts have often been disjointed, and clear policy frameworks for areas such as taxation, platform responsibilities, and informal online commerce are still evolving.

¹ This chapter was prepared by the Ethiopian local consultants based on desk research, interviews, and field observations. The content reflects the consultant's independent analysis and does not represent the official policy recommendations of the Korean advisory team.

Against this background, this section examines the current state of Ethiopia's e-commerce ecosystem by mapping key actors and infrastructure across platforms, payment systems, logistics and fulfilment services, and regulatory and policy frameworks, while also highlighting the role of the digital divide in shaping participation and access. This ecosystem-level perspective provides the contextual foundation for the subsequent analysis of technical standards and legal frameworks, which aim to address identified bottlenecks and support the development of a more coherent, trusted, and sustainable e-commerce environment in Ethiopia.

1.2.2. Key Market Players and Platforms

For Ethiopia's e-commerce ecosystem to function effectively, coordination among several core actors is essential. These include digital platforms that facilitate online transactions, payment infrastructure providers that enable secure and interoperable digital payments, and logistics and fulfilment actors responsible for warehousing, transportation, and last-mile delivery. The maturity and interaction of these actors directly shape the efficiency, reliability, and scalability of e-commerce activities in the country.

In Ethiopia, the roles and capabilities of these key players remain uneven and are strongly influenced by regulatory arrangements, digital infrastructure constraints, levels of financial inclusion, and logistics capacity. This section reviews the main market participants across platforms and payment infrastructure, highlighting recent developments, structural limitations, and their implications for e-commerce growth.

E-Commerce Platforms

A range of e-commerce platforms currently operate in Ethiopia, spanning early-stage startups and more established market players. Despite growing demand for online commerce, the sector has experienced high volatility. Several platforms that once operated in the market—such as Balesuq, Jumia, Sheger-net, and Qefira—have exited, reflecting persistent challenges related to regulatory uncertainty, payment and logistics constraints, high operating costs, and difficulties in achieving sustainable scale. These exits underscore the fragility of Ethiopia's e-commerce ecosystem and the need for a more enabling and predictable operating environment.

At the same time, a number of platforms continue to operate and attract a growing user base, each adopting distinct business models and market focuses:

- Zemen Gebeya (launched May 2025) operates as a B2C national digital marketplace connecting buyers and sellers across Ethiopia. Its model integrates online trade with digital payments—primarily via Telebirr—and logistics services targeting individuals, SMEs, and larger enterprises.

- Jiji, which expanded into Ethiopia from Nigeria in late 2020, primarily operates as a C2C classified platform while also supporting B2B listings. It facilitates listings across categories such as vehicles, property, and electronics, functioning largely as a discovery and advertising platform rather than a fully integrated transactional marketplace.
- Ashewa, founded in 2020, follows a B2B2C marketplace model linking buyers directly with micro and small enterprises and manufacturers. The platform emphasizes disintermediation and local business empowerment through digital channels.
- Afrotie/Gari, established in 2018, operates mainly as a C2C classified platform focusing on vehicles, property, electronics, and job listings across multiple cities, supporting peer-to-peer and small business transactions.
- ChipChip, founded in 2023, employs a social group-buying model connecting urban consumers with farmers and suppliers. By aggregating demand, it offers bulk-purchase discounts and focuses primarily on agricultural products and selected fast-moving consumer goods.
- MekinaNet, established in 2010, is a specialized B2C automotive marketplace enabling individuals and brokers to list vehicles for sale or rent.
- Helloomarket, founded in 2020, operates as a B2C platform linking local SMEs and producers with consumers, offering products such as leather goods, coffee, apparel, and tools, and integrating local digital payment solutions such as Hello Cash.
- Beyond formal platforms, a substantial volume of online transactions in Ethiopia takes place through informal social commerce channels, including Telegram, Facebook Marketplace, and TikTok. These channels are particularly attractive to MSMEs and individual sellers due to their low entry barriers, minimal compliance requirements, and ease of use, but they also operate largely outside formal regulatory and consumer protection frameworks.

Switch Operators

Ethiopia's digital payment infrastructure is anchored by EthSwitch, established in 2011 as a share company owned by all banks in the country and mandated by the National Bank of Ethiopia (NBE). EthSwitch functions as the sole national switching operator, providing interoperability for ATM, POS, and peer-to-peer (P2P) transactions. All fintech companies and payment service providers rely on the EthSwitch network to operate.

According to interviews with EthSwitch experts and data from the NBE Financial Stability Report, EthSwitch processed over 2.78 million interoperable POS transactions worth approximately 7.2 billion Birr in FY 2024/25, representing a 24 percent increase from the previous year. EthSwitch is also in the process of launching Ethiopia's National Payment Gateway (NPG) to support e-commerce transactions and is engaging with continental initiatives such as the AfCFTA and the Pan-African Payment and Settlement

System (PAPSS) to advance cross-border payment integration.

Another switching service provider, Premier Switch Solutions (PSS), operates as a third-party banking technology firm owned by six private banks. Established in 2009, PSS delivers shared electronic payment services to financial institutions and was the first third-party payment processor certified by the NBE. However, unlike EthSwitch, PSS does not constitute national infrastructure and depends on EthSwitch for interoperability, limiting its independent operational scope.

Table 1-2 Interoperability Through ATM, POS, and P2P Transactions, 2020–2024

	June 2020	June 2021	June 2022	June 2023	June 2024
ATM transactions					
Number	15,044,699	24,166,034	39,894,113	71,433,041	94,030,684
Value (billion birr)	12.78	26.56	44.9	89.7	119.24
POS transactions					
Number	1,107	109,506	361,317	970,434	2,345,444
Value (billion birr)	1.02	0.2	0.3	2.6	5.51
P2P transactions					
Number	0	29,881	2,067,710	14,140,881	55,204,745
Value (billion birr)	0	0.2	19.9	113.3	283.01

Source Financial Stability Report, Nov 2024, NBE²

1.2.3. Payment, Logistics, and Fulfilment Infrastructure

Payment Gateway Providers

Following the issuance of Directive No. ONPS/01/2020 on the Oversight of the National Payment System by the National Bank of Ethiopia (NBE) in March 2020, Ethiopia's digital payments landscape has expanded rapidly. The directive opened the market to non-bank payment service providers, including mobile network operators, thereby accelerating the entry of payment gateways and fintech firms into the ecosystem. This regulatory shift has played a critical role in enabling e-commerce transactions by supporting merchant onboarding, online payment acceptance, and interoperability with mobile wallets and banking systems.

At present, two payment gateway providers play a particularly prominent role in supporting e-commerce transactions in Ethiopia.

² nbe.gov.et/wp-content/uploads/2024/11/Financial-Stability-Report_NOV2024.pdf

Chapa Financial Technologies S.C. operates as an online payment gateway enabling both small businesses and large merchants to accept domestic and international payments through application programming interfaces (APIs) and its proprietary platform. Chapa currently supports more than 10,000 merchants, providing access to 18 banks, 14 payment methods, and 25 currencies. According to company-reported figures, Chapa has processed over 30 billion ETB in transaction volume, facilitated more than 100 million transactions, and completed approximately 480 million API calls, supported by a registered user base exceeding 50,000 users. These indicators reflect the rapid scaling of payment gateway services in Ethiopia following regulatory liberalization.

Arifpay Financial Technologies S.C. provides digital payment solutions through services such as ArifPOS and ArifGateway, targeting micro, small, and medium enterprise (MSME) merchants, banks, and consumers. During the 2024/25 Ethiopian fiscal year, Arifpay processed transactions exceeding 24 billion ETB. The company is also preparing to introduce additional solutions, including a Terminal Management System (TMS), aimed at strengthening merchant-side payment infrastructure and transaction management capabilities.

Together, these payment gateway providers play a critical intermediary role between e-commerce platforms, financial institutions, and end-users, enabling secure and scalable online transactions within Ethiopia's evolving digital commerce ecosystem.

Digital Wallets

Digital wallets constitute the backbone of retail digital payments in Ethiopia and are central to the functioning of e-commerce platforms. Among these, Telebirr, launched in 2021 by Ethio Telecom, is the country's largest and most widely used mobile money platform. Telebirr enables users to conduct peer-to-peer transfers, merchant payments, bill payments, online purchases, QR-code-based in-store payments, cash withdrawals via agents, and the receipt of international remittances. To date, Telebirr has processed close to 7 trillion ETB in transaction value and serves approximately 57 million subscribers, supported by 358,000 agents and 344,000 merchants nationwide. Telebirr is deeply integrated with e-commerce platforms through payment gateways, making it a dominant enabler of online transactions.

Another major digital wallet is CBE Birr, a bank-led mobile wallet operated by the Commercial Bank of Ethiopia (CBE). CBE Birr supports peer-to-peer transfers, merchant payments, salary disbursements, and utility payments, leveraging the infrastructure and trust associated with Ethiopia's largest commercial bank. As of mid-2024, CBE's total customer base reached 45 million, with 34.2 million users registered for CBE Birr services. While detailed annual growth rates are not consistently published, available figures indicate continued expansion and strong adoption.

In addition to these leading platforms, several other digital wallets operate in Ethiopia,

including M-Pesa (Safaricom Ethiopia), Awash Birr (Awash Bank), Amole (Dashen Bank), and Hello Cash (microfinance institutions). Collectively, these wallets contribute to expanding payment choice, financial inclusion, and the usability of e-commerce platforms, although interoperability and consistent user experience remain ongoing challenges.

Logistics and Fulfilment Actors

► First- and Middle-Mile Delivery

Ethiopia's most advanced first- and middle-mile logistics provider is the Ethiopian Airlines Group (ET) E-Commerce Logistics Hub, which plays a uniquely strategic role in both national and continental e-commerce logistics. Based on interviews with the ET E-Commerce Logistics Hub project management team, the facility leverages Ethiopian Airlines' cargo and logistics network to deliver goods arriving from global markets to destinations across Africa. The airline currently serves nearly 70 cargo destinations and has the capacity to handle approximately 787,006 tons of cargo annually (2024/25).

The ET E-Commerce Logistics Hub is positioned as a foundational infrastructure for cross-border e-commerce, enabling Ethiopia to function as a logistics gateway for the continent rather than solely as a domestic market participant.

► Last-Mile Delivery

Last-mile delivery services in Ethiopia remain concentrated in major urban centers, particularly Addis Ababa, and are primarily provided by local firms. Early pioneers include Deliver Addis, which established one of the country's first online food delivery platforms, and Beu-Delivery, known for rapid expansion and the use of bicycle fleets to provide cost-effective delivery services for food, pharmaceuticals, and consumer goods. Other notable actors include Zmall Delivery and Tikus Delivery, both of which manage extensive restaurant networks and have expanded into grocery and general merchandise delivery. Technology-enabled logistics providers such as Eshi-Express offer same-day and next-day parcel delivery services, often operating as dedicated partners to e-commerce platforms.

These firms play a critical role in navigating Ethiopia's urban logistics challenges, including traffic congestion and the absence of a standardized national addressing system, thereby enabling the final link between digital platforms and consumers.

► Fulfilment and Sorting

A major structural development in Ethiopia's e-commerce logistics landscape is the establishment of the ET E-Commerce Logistics Hub at Bole International Airport, described by interviewees as the first large-scale, dedicated e-commerce sorting and fulfilment facility in both Ethiopia and Africa. The facility is specifically designed to handle cross-border e-commerce, mail, and courier logistics and offers automated parcel-level

sorting, consolidation and deconsolidation, repackaging, labeling, temporary storage, and customs clearance services compliant with ICS2 standards.

The hub occupies approximately 15,000 square meters, has a handling capacity of 150,000 tons per year, and was constructed at a cost of approximately USD 55 million by a Chinese contractor. Its advanced technological systems enable end-to-end shipment tracking and position Ethiopia as a potential continental logistics hub for digital trade.

At the platform level, Ashewa operates its own logistics arm, ALEMS, providing packaging, order processing, and warehousing services for vendors. Additional firms such as Solomon Zewdu Shipping & Freight Forwarding and Pave Logistics offer general warehousing, storage, and customs clearance services that support e-commerce inventory management and broader supply chain functions.

Together, these logistics and fulfilment actors form the physical backbone of Ethiopia's e-commerce ecosystem, bridging international shipping, domestic distribution, and last-mile delivery to end consumers.

1.2.4. Market Trends and Usage Patterns

Ethiopia's e-commerce market remains relatively small by global standards; however, recent trends indicate rapid growth and expanding user adoption. Market revenue is projected to reach approximately USD 971 million in 2025, with user penetration expected to rise from about 29.8 percent in 2025 to over 31 percent by 2030. The number of e-commerce users is projected to reach nearly 18.7 million by 2030, reflecting the growing role of online commerce in Ethiopia's domestic economy. A defining characteristic of this growth is its strong reliance on mobile access, with an estimated 65 percent of online purchases conducted via mobile phones. This mobile-centric usage pattern reflects both the widespread diffusion of mobile devices and the limited availability of fixed broadband infrastructure.

From a payment perspective, mobile money has emerged as the dominant mode of transaction within Ethiopia's digital economy. Mobile wallets, led by Telebirr and complemented by bank- and fintech-led services, underpin the majority of e-commerce payments. Telebirr alone has accumulated tens of millions of registered users and processes transactions at a scale measured in trillions of birr across peer-to-peer transfers, merchant payments, and online transactions. The rapid expansion of digital finance services over recent years illustrates the critical role of interoperable payment infrastructure in enabling e-commerce growth, even as reliance on cash continues to decline gradually.

This expansion is further reflected in official transaction data published by the National Bank of Ethiopia. As summarized in [Table 1-3], the number and value of transactions

processed through digital finance services have increased sharply over recent years, underscoring the growing centrality of digital payments in everyday economic activity. These trends suggest that payment infrastructure is no longer a peripheral constraint for e-commerce growth; rather, it is becoming a foundational layer that must be supported by coherent legal, regulatory, and standards frameworks.

Table 1-3 Transaction Processed Through Digital Finance Services, 2020–2024
(numbers of transaction in millions and value in billions birr)

Year Ending		June 2020	June 2021	June 2022	June 2023	June 2024
ATM	Volume	153.19	225.60	171.07	356.38	437.98
	Value	142.07	236.09	197.54	478.32	728.51
PoS	Volume	1.36	2.95	2.34	6.60	10.15
	Value	4.85	7.44	62.18	40.84	24.24
Mobile Banking	Volume	11.62	39.56	88.01	474.92	1,114.81
	Value	68.38	326.18	163.57	3,442.58	6,717.58
Internet Banking	Volume	0.53	2.41	1.09	5.80	15.12
	Value	22.55	26.59	129.57	358.14	749.05
Agent Banking	Volume	4.24	23.00	34.39	101.95	130.35
	Value	1.40	8.94	23.01	76.54	446.00
Mobile Money	Volume	4.24	7.25	48.50	298.83	764.88
	Value	2.96	5.94	24.36	380.30	1,028.59
Aggregate DFS	Volume	175	301	345	1,244	2,473
	Value	242.20	611.18	1,600.24	4,776.72	9,693.97

Source National Bank of Ethiopia (NBE)

Logistics trends present a more mixed picture. Ethiopia's logistics and fulfillment sector is still at an early stage of development, and limitations in last-mile delivery remain a key constraint on e-commerce expansion. Average delivery times are estimated at two to three days within Addis Ababa, compared to seven to ten days for destinations outside the capital. Despite these challenges, the e-commerce logistics market is expanding rapidly. The market was valued at approximately USD 546 million in 2024 and is projected to grow to over USD 1.6 billion by 2033, reflecting rising demand for delivery, warehousing, and fulfillment services linked to online trade. This growth trajectory highlights both the scale of unmet demand and the importance of continued investment in logistics infrastructure and coordination.

At the same time, persistent digital divides continue to shape usage patterns and constrain the inclusiveness of e-commerce growth. Disparities in internet access,

smartphone ownership, and digital skills—across gender, income levels, and urban–rural residence—remain significant. Sub-Saharan Africa records the lowest levels of internet usage globally, and Ethiopia reflects many of these regional characteristics. While connectivity is improving, uneven access to devices, affordable internet services, and digital financial tools limits the ability of large segments of the population to participate fully in e-commerce markets. These structural constraints underscore that market growth alone is insufficient; addressing the digital divide is essential to ensure that the expansion of e-commerce translates into inclusive and sustainable economic participation.

1.2.5. Digital Divide and Inclusion Challenges

The digital divide remains a significant structural constraint on the development of e-commerce in Ethiopia. While digital connectivity and mobile phone usage have expanded rapidly in recent years, access to digital services—and the ability to participate meaningfully in online markets—remains uneven across population groups. These disparities shape who can engage in e-commerce, under what conditions, and at what scale.

At a regional level, Sub-Saharan Africa continues to record the lowest levels of internet usage globally, reflecting persistent infrastructure gaps and affordability constraints. Ethiopia shares many of these regional challenges, which manifest in differentiated access across age, gender, geography, and disability status.

Age and Usage Patterns

Ethiopia's population is young and increasingly connected, with rising mobile phone penetration and internet usage supporting the expansion of digital services. Younger users, in particular, are driving e-commerce adoption through informal social marketplaces such as Telegram, Facebook, and Jiji. However, available data suggest that age itself is not the primary determinant of exclusion. Smartphone ownership rates across age groups are relatively similar, indicating that factors such as income, education, digital literacy, and infrastructure play a more decisive role in shaping unequal participation in e-commerce.

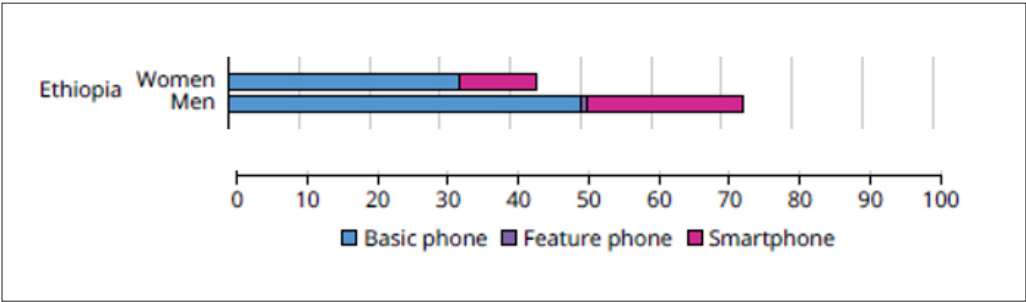
Gender Gaps in Devices and Financial Inclusion

Gender-based disparities remain a critical dimension of digital exclusion. Although recent indicators suggest that women in Ethiopia may not be significantly disadvantaged in basic internet access, this apparent parity masks deeper structural barriers. Women are less likely than men to own smartphones, which are the primary devices used for

accessing e-commerce platforms, digital marketplaces, and mobile payment services. Lower device ownership therefore constrains women's effective participation in online commerce.

These challenges are compounded by persistent gaps in financial inclusion. While the gender gap in account ownership has narrowed in recent years, women continue to represent a disproportionate share of unbanked adults. Without access to bank accounts or mobile money services, participation in e-commerce—whether as consumers or sellers—remains limited. Addressing gender disparities in e-commerce thus requires policy interventions that extend beyond connectivity, encompassing device affordability, digital skills, and access to formal financial services.

Figure 1-1 Ethiopian Adults with a Mobile Phone (%) 2024



Source Open Knowledge Repository, World Bank

Urban–Rural Divide

Geographic disparities present another major constraint. Urban residents are significantly more likely to own smartphones and access digital services than their rural counterparts. In Ethiopia, where more than three-quarters of the population lives in rural areas, this divide poses a substantial challenge to inclusive e-commerce development. Excluding rural populations from digital markets would undermine the objectives of Ethiopia's national digital transformation strategies, which identify e-commerce as a key pillar. Recent policy commitments, including investments in rural electrification and connectivity under the Digital Ethiopia 2030 agenda, reflect growing recognition of this challenge.

Inclusion of Persons with Disabilities

Digital exclusion is particularly pronounced among persons with disabilities. Across Sub-Saharan Africa, individuals with disabilities consistently report lower levels of device ownership, digital skills, and internet use. Barriers include both affordability constraints and the absence of accessible technologies, such as screen readers and assistive

interfaces. In Ethiopia, where a significant share of the population lives with disabilities, these limitations further restrict participation in digital services and e-commerce. Inclusive digital trade strategies will therefore need to incorporate accessibility considerations alongside broader connectivity and affordability measures.

Taken together, these dimensions of the digital divide underscore that expanding e-commerce in Ethiopia is not solely a matter of platform availability or payment infrastructure. Meaningful participation depends on addressing structural inequalities in access to devices, skills, financial services, and enabling infrastructure. Without targeted inclusion measures, the benefits of e-commerce growth are likely to remain concentrated among already-connected populations.

1.2.6. Regulatory and Policy Environment

Ethiopia's regulatory and policy environment for e-commerce has evolved significantly in recent years, reflecting broader national efforts to promote digital transformation, financial inclusion, and secure electronic transactions. While the legal framework remains under development in several areas, recent policy initiatives provide an important institutional foundation for the growth of digital commerce.

Digital Payments Policy Framework

Ethiopia has taken concrete steps to expand the use of digital payments and reduce reliance on cash-based transactions. In May 2025, the Ministry of Finance issued Directive No. 1069/2025, requiring all federal public institutions to accept payments from any licensed digital payment service provider, including mobile wallets, bank transfers, prepaid instruments, and cards, without discrimination among providers. This directive aims to promote financial inclusion, enhance competition among payment service providers, and normalize the use of digital payments in public-sector transactions.

These regulatory measures are complemented by Ethiopia's National Digital Payments Strategy 2026–2030, which outlines a long-term roadmap for developing an inclusive, interoperable, and secure digital payments ecosystem. The strategy places particular emphasis on instant payment systems and explores pathways toward low-value cross-border retail payment integration, aligning domestic payment reforms with Ethiopia's broader digital economy objectives.

E-Commerce and Electronic Transactions Legislation

The principal legal instrument governing electronic commerce and related digital transactions in Ethiopia is the Electronic Transactions Proclamation (No. 1205/2020), which entered into force in June 2020. This proclamation establishes the legal validity

of electronic records and electronic signatures, thereby providing the foundational legal certainty required for online transactions. It also introduces obligations for e-commerce intermediaries related to secure data handling and embeds consumer protection considerations applicable to digital platforms.

While the proclamation offers a general legal basis for electronic transactions, it does not address several e-commerce–specific regulatory issues in detail. As a result, the current legal framework provides broad enabling principles rather than operational guidance for platform governance, intermediary responsibilities, and market entry conditions.

Data Governance and Cybersecurity

Recent developments in data protection and cybersecurity have further shaped Ethiopia's digital policy landscape. In July 2024, Ethiopia enacted the Personal Data Protection Proclamation (No. 1321/2024), which introduces core data protection rights, including rights of access, rectification, erasure, and breach notification. The law also establishes conditions for lawful data processing and cross-border data transfers, subject to appropriate safeguards.

Despite this progress, implementation challenges remain. Enforcement mechanisms and detailed regulatory guidelines are still under development, and public awareness of data protection rights remains limited. Cybersecurity continues to be identified as a strategic priority within Ethiopia's digital transformation agenda, with ongoing efforts focused on strengthening institutional capacity, developing technical expertise, and enhancing cooperation between public and private actors to address emerging digital risks and protect critical infrastructure.

Taken together, Ethiopia's regulatory and policy environment provides an emerging foundation for e-commerce development. While key legal and policy instruments are in place, further clarification and operationalization will be required to translate these frameworks into effective governance mechanisms for the digital marketplace.

1.2.7. Practical Gaps and Emerging Opportunities

Despite notable progress in digital payments, connectivity, and policy formulation, Ethiopia's e-commerce ecosystem continues to face a number of practical constraints that limit its scalability, reliability, and inclusiveness. These constraints are not isolated issues, but rather structural gaps that cut across regulatory design, institutional coordination, market readiness, and trust mechanisms.

Legal and regulatory gaps remain a central challenge. While Ethiopia has enacted several proclamations and directives relevant to electronic transactions and digital

payments—including the Electronic Transactions Proclamation and the National Payment System framework—these instruments do not yet comprehensively address the operational realities of e-commerce. Existing regulations tend to focus disproportionately on payment transactions, leaving critical dimensions such as logistics and fulfilment, returns and dispute resolution, platform responsibilities, consumer protection, cybersecurity, interoperability, and technical standards only partially covered. In addition, taxation and informal online commerce conducted through social media platforms such as Telegram, Facebook, and TikTok remain largely outside the formal regulatory perimeter. The absence of a dedicated regulatory or innovation sandbox for e-commerce has further constrained experimentation, compliance learning, and ecosystem-wide coordination.

Logistics and fulfilment constraints present another major bottleneck. Interviews with key stakeholders highlight persistent challenges related to last-mile delivery, unreliable addressing systems, high delivery costs, and weak coordination among logistics service providers. For cross-border e-commerce in particular, unclear customs procedures and limited facilitation mechanisms continue to raise transaction costs and operational uncertainty, affecting Ethiopia's ability to leverage emerging logistics hubs and regional connectivity.

Digital divide challenges continue to shape unequal participation in e-commerce. Disparities in internet access, smartphone ownership, digital literacy, and access to digital financial services—across gender, income, and urban–rural dimensions—exclude significant segments of the population from online markets. Without targeted and sustained interventions, these inequalities risk reinforcing existing socioeconomic divides and limiting the inclusiveness of e-commerce growth.

Institutional fragmentation also constrains ecosystem development. The absence of a dedicated central coordinating body for e-commerce has resulted in fragmented policy efforts and weak inter-agency coordination among regulators, platforms, payment service providers, logistics operators, and merchants. This fragmentation complicates the implementation of cross-cutting reforms and slows the translation of policy objectives into operational outcomes.

At the market level, merchant readiness and onboarding capacity remain uneven. Many merchants—particularly micro and small enterprises—face barriers related to limited digital skills, weak record-keeping practices, informality, and resistance to platform requirements on pricing transparency, quality standards, taxation, and consumer protection. These constraints reduce platform participation and limit the depth of the online marketplace.

Trust deficits further undermine ecosystem growth. Opportunistic behavior by both sellers and buyers, combined with weak enforcement mechanisms and limited dispute-resolution frameworks, has eroded confidence in online transactions. Strengthening digital identity-based verification mechanisms, including the use of Ethiopia's national

digital ID system (Fayda), offers a potential pathway to improving accountability, reducing fraud, and reinforcing trust across platforms.

At the same time, Ethiopia possesses several emerging opportunities that provide a foundation for future e-commerce development. The establishment of the Ethiopian Airlines Group's E-Commerce Logistics Hub represents a significant infrastructural asset, offering large-scale sorting, fulfilment, and cross-border logistics capabilities that are rare on the continent. Similarly, EthSwitch has laid important groundwork for payment interoperability through national switching infrastructure, interoperable QR standards, and initiatives such as Ethiopay, under the regulatory oversight of the National Bank of Ethiopia.

Taken together, these gaps and opportunities underscore a central conclusion: Ethiopia's primary challenge is not the absence of digital ambition, but the need to consolidate foundational legal, technical, and institutional elements into a coherent e-commerce framework. Addressing regulatory clarity, transaction assurance, platform responsibilities, and trust mechanisms emerges as a necessary precondition for scaling the ecosystem and translating existing infrastructure investments into sustainable market outcomes.

Standardization Framework for Transaction Assurance

Transaction assurance is a foundational element for building trust in e-commerce, particularly in markets where the digital economy and consumer trust mechanisms are still in the early stages of development. E-commerce transactions span multiple actors, technologies, and processes across upstream and downstream phases of the digital marketplace. These interconnected elements increase the likelihood of vulnerabilities arising throughout the transaction lifecycle—from product information disclosure and customer authentication to payment processing, delivery, and post-transaction dispute resolution. Ensuring reliability and trust in this environment requires attention, coordination, and accountability from all stakeholders, including government agencies, platform operators, service providers, and consumers.

This chapter provides policy-oriented consultation for developing a national framework that assures trustworthy e-commerce transactions in Ethiopia's e-commerce ecosystem. Drawing on global best practices and key principles embedded in international standards, it identifies and prioritizes core elements that can enhance transaction reliability. It also reviews recent developments in Ethiopia's e-commerce trust initiatives and explores how national standards can evolve into practical mechanisms, such as voluntary certification schemes or trust mark programs for digital platforms. The outcomes of this chapter aims to provide a structured foundation for policy recommendations and implementation procedures to foster a trustworthy e-commerce environment in Ethiopia.

2.1. Overview : Standards as a Policy tool for e-Commerce Trust Assurance

2.1.1. Trust Challenges in e-Commerce Transaction

Trust is the cornerstone of any functioning e-commerce ecosystem. Unlike traditional commerce, where buyers can physically examine products and directly interact with sellers, e-commerce transactions are characterized by distance, intangibility, and information asymmetry. Consumers must rely on digital interfaces, unseen logistics systems, and institutional guarantees rather than personal judgment. In such environments, transaction assurance—the ability to guarantee that each step of an online transaction is carried out reliably, securely, and transparently—becomes essential for building and sustaining trust.

This is particularly important in markets where the digital economy is still in its early stages of development. In such contexts, consumers are less familiar with online purchasing, businesses may lack standardized operating procedures, and regulatory institutions are still building capacity. Consequently, transaction risks—such as product misrepresentation, payment fraud, data misuse, delivery failure, or absence of dispute resolution—tend to be higher and more visible to the public. If these vulnerabilities are left unaddressed, consumer confidence declines rapidly, discouraging adoption and limiting market growth.

E-commerce transactions typically pass through multiple stages—pre-purchase (information search, seller credibility assessment), purchase (payment, authentication), and post-purchase (delivery, return, dispute resolution). Each stage contains uncertainties. Thus, assuring reliability across the transaction lifecycle is critical not only for protecting consumers but also for enabling platforms to scale, attract investment, and integrate into global value chains.

The following structural challenges affecting consumer trust and transaction assurance in the e-commerce landscape, particularly in early-stage markets such as Ethiopia, are summarized in [Table 2-1].

Table 2-1 Trust challenges in e-Commerce Transactions

Challenge Area	Description
Unknowns in the purchasing process	Consumers lack full information on sellers, product authenticity, delivery reliability, and data security.
Product quality & IPR concerns	Counterfeit goods, ambiguous quality standards, and weak enforcement of intellectual property rights undermine trust.

Personal data protection	Absence of clear privacy standards and data handling protocols increases risk of misuse or cyber breaches.
After-sale services	Limited refund, return, or repair mechanisms reduce willingness to transact online.
Transaction security	Payment fraud, unreliable gateways, and lack of escrow services increase perceived risk.
Logistics and delivery	Delays, damaged goods, or non-delivery reduce user confidence and platform credibility.

Source compiled by author

E-commerce transaction assurance refers to the institutional, technical, and operational mechanisms that guarantee the integrity of transactions. It ensures: 1) Products are delivered as described; 2) Payments are secure and traceable; 3) Consumer data is protected; 4) Platforms follow transparent procedures; 5) Disputes are resolved fairly and efficiently.

These assurances form the backbone of consumer trust. When they are absent or weak, trust quickly deteriorates; no level of advertising, platform design, or legal measures can sustain user engagement if consumers believe that platforms cannot deliver on their promises. In contrast, when platforms demonstrate compliance with clear standards, independent certifications, and reliable dispute resolution mechanisms, trust becomes institutionalized and scalable rather than dependent on individual seller reputation or personal experience.

2.1.2. Standards as a Policy Tool for e-Commerce Transaction

Addressing the complexity of digital transactions requires governments and regulators to implement a range of policy instruments to foster trust, as summarized in [Table 2-2]. These instruments may include legal frameworks, financial incentives, assurance and certification systems, consumer education, and dispute resolution mechanisms.

Hard law and licensing—such as proclamations or mandatory registration of e-commerce platforms—provide legal enforceability and formalize market entry. However, they tend to be resource-intensive and slow to adapt to technological changes. Fiscal instruments, including VAT exemptions and subsidies for logistics or digital infrastructure, can stimulate market participation, particularly for small and medium enterprises, but they depend heavily on national budget capacity. Educational initiatives and awareness campaigns expand digital literacy and inform consumers about their rights, but behavioral change takes time and depends on consistent implementation. Alternative dispute resolution systems—such as escrow mechanisms, online mediation

boards, or transaction insurance—reduce the cost and friction of resolving conflicts but require institutional capacity and financial trust funds to function credibly.

Among these tools, standards and certification mechanisms hold unique value for transaction assurance in e-commerce. Unlike rigid legal instruments, standards are voluntary guidelines that structure market behavior without imposing excessive regulatory burdens. They help define what constitutes a secure payment process, what minimum data protection measures should be followed, how platforms should present product information, or what level of service is required for customer support. When combined with third-party certification or trust marks, standards provide measurable evidence of compliance and make trust visible rather than abstract. They are also adaptable, can be updated more easily than legislation, and align domestic industries with international expectations—an essential feature for countries seeking to participate in regional or global digital trade such as Ethiopia.

Table 2-2 Policy Tools: Trust-building for e-Commerce Transaction

Policy Tool	Typical Use	Strengths	Limitations
Hard law & licensing	Proclamations, mandatory licensing of platforms	Strong legal enforceability	Slow to update; resource-intensive enforcement
Taxes & incentives	VAT relief, logistics subsidies	Direct economic impact	Dependent on public budget
Standards & certification	Voluntary codes, combined with a third-party trust mark	Flexible, market-driven, export-friendly	Requires credible auditors; low uptake without incentives
Education & awareness campaigns	Digital literacy, consumer protection outreach	Quick implementation, public visibility	Behavior change is uncertain
ADR (Alternative Dispute Resolution) & insurance	Online dispute boards, escrow, transaction insurance	Reduces conflicts and increases confidence	Needs trust funds, legal backing, and skilled arbitrators

Source compiled by author

Standards can be defined as a set of specifications to which all elements of products, processes, formats, or procedures must conform. According to the WTO Agreement on Technical Barriers to Trade,³ a standard is “a document approved by a recognized body that provides, for common and repeated use, rules, guidelines or characteristics for products or related processes and production methods.” Standardization, in turn, refers to the process

³ https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm

by which conformity to these specifications is established and maintained. ISO/IEC (2004)⁴ defines it as the “activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context.” In practical terms, standards describe what “good practice” looks like, and standardization is the systematic coordination among different actors—governments, platforms, logistics providers, payment intermediaries, and auditors—to ensure that these practices are consistently implemented.

Standards play a critical role in fostering trust in e-commerce by fulfilling several key functions, as summarized in [Table 2-3]. First, they enhance information transparency by reducing information asymmetry between buyers and sellers; consumers can compare platform practices and product information more easily, while firms adopt clearer documentation and disclosure procedures. Second, standards contribute to variety reduction and economies of scale by encouraging the use of uniform formats, terminology, and processes, which lowers operational costs and facilitates wider market participation. Third, they embed quality and safety requirements into transactions, helping ensure that goods, services, and digital operations meet minimum performance, reliability, and sustainability criteria. Fourth, they enable compatibility and interoperability across systems—for example, ensuring that payment gateways, digital identities, and logistics tracking systems can interact seamlessly. This interoperability unlocks network effects, where the value of participation increases as more actors adopt the same standard. Fifth, standards help reduce transaction costs by lowering the need for repeated negotiation, verification, or monitoring; expectations are predefined and mutually understood. Finally, they mitigate negative externalities, for example by promoting cybersecurity, ethical data practices, and environmentally responsible logistics.

Table 2-3 Role of Standards in e-Commerce Trust Assurance

Function of Standards	Contribution to Trust & Market Development
Information / Transparency	Reduce information asymmetry, allow consumers to compare services, and support technology transfer
Variety Reduction & Economies of Scale	Standardized formats and processes lower production costs and expand market participation
Quality & Safety Assurance	Embed minimum performance, safety, sustainability, and service quality requirements
Compatibility & Interoperability	Allow systems (payment gateways, logistics data, APIs) to work together, enabling network effects
Transaction Cost Reduction	Reduce negotiation, verification, and monitoring costs by providing predefined expectations
Correcting Negative Externalities	Address cyber risk, environmental impact, unfair practices

Source Blind (2013)⁵

Standards are particularly effective for e-commerce trust because they make trust measurable, visible, and auditable. Through documentation, inspection, and certification, platforms can externally demonstrate their trustworthiness to consumers, business partners, and regulators. They remove ambiguity about what constitutes a “safe,” “reliable,” or “ethical” platform and instead translate these values into operational criteria. Moreover, internationally harmonized standards reduce transaction costs in cross-border trade and facilitate Ethiopia's participation in frameworks such as the African Continental Free Trade Area (AfCFTA)'s digital protocol. Research has shown that strong national standard systems positively influence export performance by signaling quality and compliance (Blind & Jungmittag, 2000). Platforms that adopt global standards—such as ISO/IEC standards, the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) recommendations,⁶ or web accessibility guidelines—can more easily integrate into international supply chains and meet the expectations of foreign consumers and investors.

In sum, trust is a precondition for the growth of e-commerce. Transaction assurance is the mechanism through which trust is operationalized across the entire lifecycle of digital transactions. Ethiopia possesses strong policy momentum, but institutional mechanisms and standard-based frameworks are necessary to translate vision into reliable practice. Standards provide one of the most effective tools to achieve this goal: they are flexible, scalable, internationally recognized, and capable of reducing transaction costs while aligning stakeholders around shared principles. Going forward, policy implementation should focus on technical infrastructure, adoption of standards, and capacity-building across public and private actors to create an environment in which e-commerce can thrive sustainably.

2.2. Consideration for Transaction Assurance: Key International Standards

E-commerce transaction assurance is increasingly shaped by interactions that go beyond national boundaries. As digital transactions involve sellers, buyers, platforms, and logistics providers across different jurisdictions, many of the risks and expectations

⁴ <https://www.iso.org/standards.html>

⁵ Blind, K. (2013). “The Impact of Standardization and Standards on Innovation”. . Nesta Working Paper 13/15 November 2013. https://media.nesta.org.uk/documents/the_impact_of_standardization_and_standards_on_innovation.pdf

⁶ Trade Facilitation and E-business (UN/CEFACT) <https://unece.org/trade/unecefact>

around trust are no longer confined to domestic policy settings. In this context, countries that are developing their own transaction assurance frameworks often look to international principles and practical experiences—not as rigid templates to be copied, but as useful references for shaping approaches that fit local conditions while remaining compatible with broader digital trade environments.

Among the international initiatives relevant to e-commerce transaction assurance, the work of the International Organization for Standardization (ISO) provides an important reference point. ISO is an independent, non-governmental international body composed of national standardization organizations from over 160 countries. It develops voluntary international standards to support compatibility, safety, and quality across industries, including emerging areas of digital trade. To understand the key elements of e-Commerce transaction assurance, we review ISO's major standardization efforts on this regard.

2.2.1. ISO Technical Committee 321: Transaction Assurance in E-commerce

Within ISO, Technical Committee 321 (ISO/TC 321) is specifically responsible for standardization related to transaction assurance in e-commerce.⁷ ISO/TC 321 was established to develop international standards that address the upstream and downstream processes of e-commerce transactions. Its scope covers a wide spectrum of transaction-related risks and assurance mechanisms, reflecting the reality that trust is not created at a single point in the transaction but must be safeguarded across the entire lifecycle of an online purchase.

The Secretariat for ISO/TC 321 is Standardization Administration of China (SAC). There are currently 16 members to this committee, including 6 African countries including DR Congo, Cote d'Ivoire, Kenya, Mali, Mauritius, Rwanda, Senegal.⁸ There are currently 21 observing countries, including 2 African countries, namely Cameroon and Nigeria.

The committee's mandate includes four major dimensions: 1) assurance of the transaction process itself; 2) protection of online consumer rights; 3) interoperability of inspection data for cross-border commerce; and 4) assurance of final delivery to the consumer.

First, transaction process assurance refers to ensuring that consumers can access e-commerce platforms easily and that commercial transactions are carried out under transparent, fair, and secure conditions. This encompasses platform entry, product

⁷ ISO/TC 321 Transaction assurance in E-commerce. <https://www.iso.org/committee/7145156.html>

⁸ China (SAC), The Democratic Republic of the Congo (OCC), Côte d'Ivoire (CODINORM), France (AFNOR), Germany (DIN), India (BIS), Japan (JISC), Kenya (KEBS), Mali (AMANORM), Mauritius (MSB), Norway (SN), Rwanda (RSB), Saudi Arabia (SASO), Senegal (ASN), Singapore (SSC), United Kingdom (BSI)

listing, consumer authentication, payment processing, and record-keeping.

Second, consumer protection is considered a core pillar of transaction assurance. ISO/TC 321 emphasizes both preventive measures—such as accurate product information, fair contract terms, and secure data handling—and reactive mechanisms, including dispute resolution and redress procedures. By incorporating both prevention and resolution, the standard highlights that consumer trust depends not only on reducing risks but also on ensuring that when problems occur, they can be resolved efficiently.

Third, ISO/TC 321 addresses a challenge specific to cross-border e-commerce: the interoperability and admissibility of inspection data for product quality. In international trade, verifying whether a product meets safety, health, or quality standards becomes complicated when inspection results are generated in one country but need to be trusted in another. By proposing a standardized approach to inspection data formats and mutual recognition mechanisms, ISO/TC 321 contributes to reducing disputes at customs, accelerating clearance processes, and fostering trust among trading partners.

Lastly, the scope includes assurance of delivery to the final consumer, acknowledging that trustworthy logistics—timely delivery, package integrity, and transparent tracking—is an indispensable part of transaction reliability.

Two standards developed under TC/321 are particularly relevant: 1) ISO 32111 (2023) Principles and Framework, and 2) ISO 32112 (2025) Relevant factors of evaluation and selection of indicators. Below we review these two standards.

2.2.2. ISO 32111:2023 Principles and Framework for Transaction Assurance in E-commerce⁹

The first published standard, ISO 32111:2023, provides the fundamental Principles and Framework for Transaction Assurance in E-commerce. It introduces a conceptual structure for understanding how trust is built and maintained across online transactions, defines key terminology, and identifies essential principles such as fairness, authenticity, accountability, accessibility, security, and privacy. The document serves as a baseline reference for governments, platforms, and certification bodies seeking to design assurance mechanisms or policy frameworks that are consistent with internationally recognized best practices, while still adaptable to local conditions.

Notably, it provides a structured framework built upon three interrelated components: Principles, Assurance Elements, and Participants. Principles provide guidance for participants on how to participate in activities during the transaction process and protect

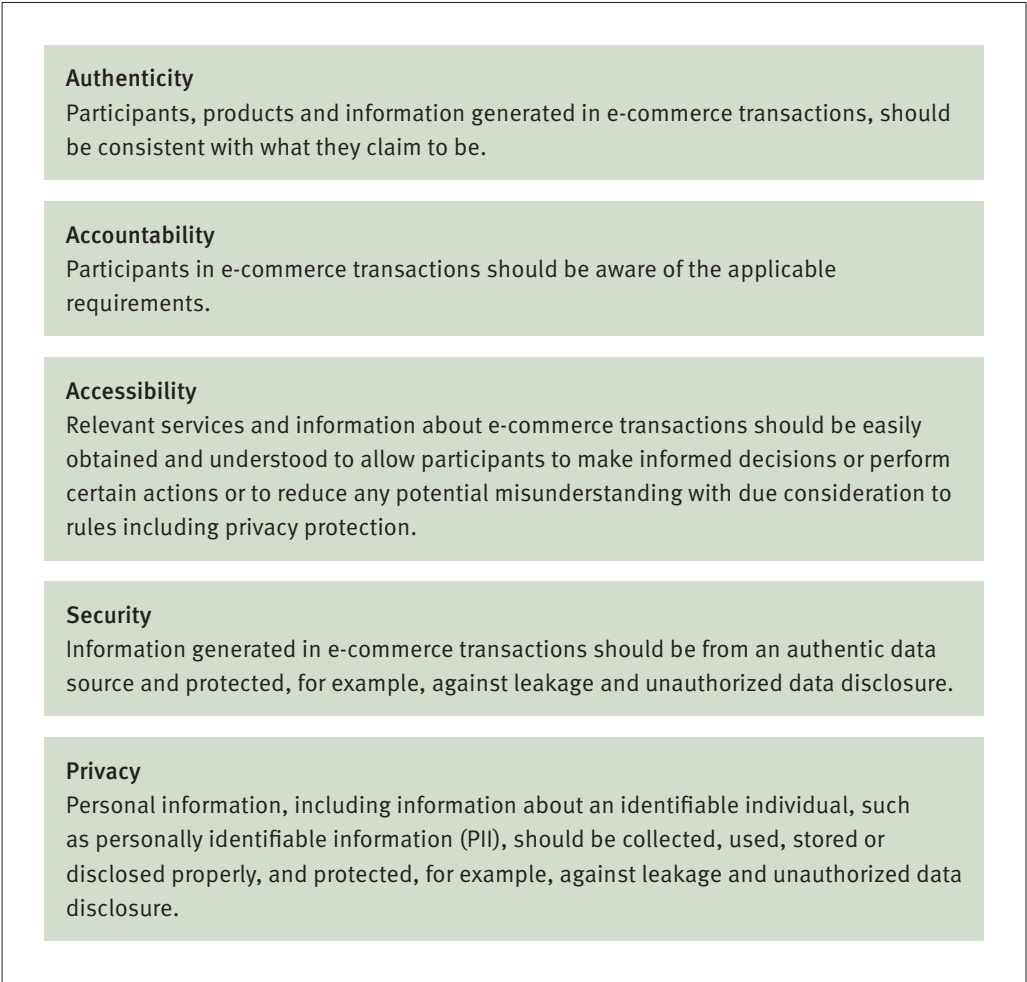
⁹ This sub-section explains the contents of the ISO 32111:2023. <https://www.iso.org/standard/80876.html?browse=tc>

their interests, and for the smooth operation of activities in e-commerce transactions. Assurance elements are those key consideration points to support the accomplishment and realization of the principles. Participants refer to those engaging in activities during the transaction process according to their responsibilities and demands.

Principles of Transaction Assurance

ISO 32111 organizes transaction assurance around several guiding principles that aim to protect the interests of all participants while ensuring the smooth operation of e-commerce activities.

Figure 2-1 ISO32111:2023—Principles of Transaction Assurance



Source ISO 32111 (2023)

Authenticity refers to the expectation that all parties, products, and information involved in e-commerce transactions should correspond to what they claim to be. This applies to seller identity, product specifications, and transaction records, ensuring that the information available to users is truthful and verifiable.

Accountability emphasizes that all participants in e-commerce transactions should understand and comply with relevant rules and responsibilities. Information generated throughout the transaction—from contract formation to dispute settlement—should be recorded and stored appropriately. This allows responsibilities to be traced and supports the resolution of disputes when they arise.

Accessibility means that information and services related to the transaction should be easy to obtain and understand. Consumers should be able to access product descriptions, terms of service, payment information, delivery status, and contact channels for support without difficulty. This also includes consideration of local regulations on accessibility and protection of personal data.

Security focuses on safeguarding data, transaction records, and system operations from unauthorized access, leakage, or manipulation. Software systems and operational processes should be protected against current and potential threats, and regular updates or security advisories should be incorporated into platform management.

Privacy addresses the handling of personal data. Information relating to identifiable individuals must be collected, used, and stored in a manner that respects privacy rights and conforms to applicable legal requirements.

These principles provide the normative foundation upon which assurance mechanisms—such as certification schemes, auditing procedures, or platform policies—can be developed.

Participants and Their Roles

ISO 32111 identifies multiple actors involved in the transaction assurance process. These include sellers, buyers, e-commerce platform operators, logistics service providers, payment service providers, software developers, manufacturers, rights holders, and collection agents. In addition, the standard highlights the role of neutral parties—such as auditors or certification bodies—responsible for reviewing compliance and issuing assurance marks where applicable.

Participants are categorized not only by their function but also by their involvement in transaction activities. Some actors initiate specific actions (for instance, a buyer placing an order or a seller confirming shipment), while others are engaged in supporting roles, such as payment processors or logistics companies. This distinction helps clarify responsibilities, risk points, and assurance requirements within different stages of the transaction.

Table 2-4 ISO32111:2023—Participants and their Roles

Participant	Role and Responsibility in Transaction Assurance
Seller	Provides accurate product or service information, ensures product quality, fulfills orders, and responds to consumer claims or disputes in accordance with platform policies and legal obligations
E-commerce Platform Operator	Operates and manages the digital platform, sets and enforces transaction rules, verifies seller identity, protects consumer data, maintains transaction records, and supports dispute resolution mechanisms
Buyer	Initiates the purchase, provides accurate personal and payment information, complies with platform policies, and confirms receipt or raises issues for post-transaction redress when necessary
Logistics Service Provider	Handles packaging, shipping, and delivery of goods; provides tracking information; ensures products are delivered in proper condition and within agreed timeframes; reports delivery exceptions
Third-party Payment Service Provider	Facilitates secure and traceable payment; ensures authentication of financial transactions; protects sensitive financial data; processes refunds or chargebacks when disputes arise
Software Service Provider	Develops or maintains software systems used by the platform or other participants (e.g., shopping cart systems, APIs, security modules) and ensures system integrity, security updates, and interoperability
Collection Agent for Goods	Acts as an intermediary who collects goods from sellers or warehouses and transfers them to logistics providers or consumers, ensuring accurate handling, documentation, and accountability
Manufacturer	Produces goods according to quality, safety, and compliance standards; provides correct product specifications; supports traceability should safety issues, defects, or recalls arise
Rights Holder	Owns intellectual property rights to products, trademarks, or digital content; verifies authorized sales; may request removal of counterfeit or infringing goods and supports enforcement of IP compliance
Neutral Party (Auditor / Certification Body)	Independently evaluates whether platform operations, data protection, logistics, and transaction procedures comply with applicable standards; issues certification or trust marks where appropriate; monitors ongoing conformity

Source ISO 32111 (2023)

Activities

Transaction assurance in ISO 32111 is structured across three main phases:

- Pre-transaction phase, where buyers and sellers prepare for engagement. This includes product listing, identity verification, disclosure of terms, and the technical readiness of platforms.
- In-transaction phase, which begins when an order is placed and continues through payment processing, order confirmation, shipment, and receipt of goods.
- Post-transaction phase, which occurs after the buyer has received the product. This stage involves confirmation of delivery, after-sale services, return and refund processes, and dispute resolution.

Each phase contains activities involving different participants, and assurance mechanisms must be tailored to these activities. Some activities are optional depending on the nature of the product or service, while others—such as payment, delivery, and information exchange—are common to most e-commerce transactions.

Figure 2-2 ISO32111:2023—Activities during the Transaction Process

- in charge
- in support

Activities during the transaction process	Participants in e-commerce transactions	Seller	E-commerce platform operator	Buyer	Third-party payment service provider	Logistics service provider	Software service provider	Collection agent for goods	Manufacturer	Rights holder
Pre-transaction phase (7.2)										
Account registration (7.2.2)		●	○	●			○		○	○
Verification of registered Information (7.2.3)		●	●	●					○	○
Preparation of third-party service (7.2.4)			●		○	○	○			
Releasing transaction-related information (7.2.5)		●	●	●	○	○	○	○	○	○
In-transaction phase (7.3)										
Placement of electronic order (7.3.2)		○	○	●						
Confirmation of electronic order (7.3.3)		●	○	●						
Choice of payment method(7.3.4)		○	○	●	○					
Payment for purchased products(7.3.5)		○	○	●	○					
Delivery of purchased products(7.3.6)		●	○	○		○		○	○	
Customs clearance(7.3.7)		●	○	○		○				
Receipt with confirmation (7.3.8)		○	○	●	○	○		○	○	
Post-transaction phase (7.4)										
Performance evaluation (7.4.2)		●	○	●	●	●				
Resolving disputes (7.4.3)		●	○	●	●	●			●	●
Return of products (7.4.4)		○	○	●		○		○	○	
Refund of payment (7.4.5)		●	○	●	○					
Compensation for transaction loss (7.4.6)		●	●	●	●	●			●	●
Maintenance and technical support (7.4.7)		●	○	○					●	

Source ISO 32111 (2023) p.5

Assurance Elements

ISO 32111 introduces assurance elements as practical tools that support the implementation of the principles. These elements help participants identify potential risks during transaction activities, take measures to mitigate them, and document compliance where necessary. Assurance elements are associated with activities throughout the e-commerce transaction process; they span the entire transaction lifecycle and can include secure payment protocols, product traceability systems, standardized delivery documentation, audit trails, and grievance mechanisms.

Figure 2-3 ISO32111:2023—Assurance Elements and Participants

Assurance elements	Participants in e-commerce transactions								
	Seller	E-commerce platform operator	Buyer	Third-party payment service provider	Logistics service provider	Software service provider	Collection agent for goods	Manufacturer	Rights holder
Identity information (8.2)	○	●	○			○			
Qualification information (8.3)	○	●	○			○		○	○
Terms of use (8.4)	○	●		○	○	○			
Third-party service rule (8.5)	○	●		○	○	○			
Online reputation information (8.6)	○	●	○	○	○				
Product information (8.7)	●	●						○	○
Transaction document (8.8)	○	●	○	○	○		○		
Multiple payment methods (8.9)	○	●		●					
Payment security rule (8.10)	○	●	○	●					
Delivery rule (8.11)	○	●			●		○	○	
Customs clearance rule (8.12)	○	○	○		○				
Performance evaluation rule (8.13)	○	●	○	○	○				
Dispute resolution rule (8.14)	○	●	○	○	○			○	○
Return and refund rules (8.15)	●	●		○	○		○	○	
Compensation rules (8.16)	○	●	○	○	○			○	○
Maintenance and technical support rule (8.17)	●	○						●	

Source ISO 32111 (2023) p.11

2.2.3. ISO 32112:2025 Relevant Factors of Evaluation and Selection of Indicators¹⁰

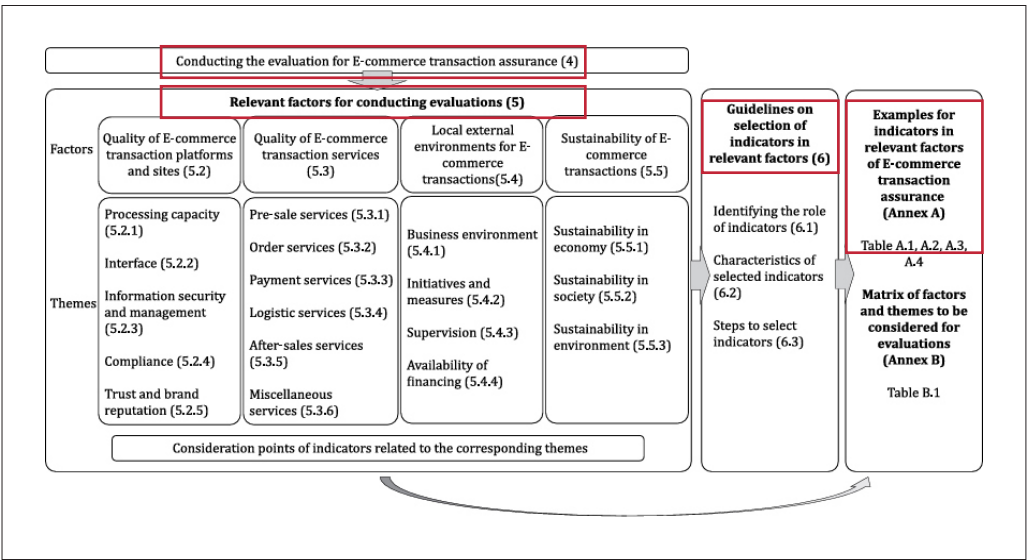
ISO 32112:2025 is designed as a complementary standard to ISO 32111, providing a structured methodology to evaluate how effectively transaction assurance is implemented in e-commerce. While ISO 32111 establishes principles and assurance elements, ISO 32112 offers a framework for measuring whether these elements operate in practice and

how they contribute to the overall reliability of e-commerce ecosystems.

The purpose of evaluation as defined in ISO 32112 is threefold. First, it provides quantitative and qualitative references that can be used by governments, platforms, auditors, and other interested parties when assessing e-commerce performance. Second, it helps identify vulnerabilities and risks across the transaction process so that corrective actions can be taken before they evolve into systemic failures. Third, it enables the detection of areas where improvements can foster sustainability, user trust, innovation, and resilience. To achieve this, ISO 32112 proposes that evaluation should be comprehensive, covering pre-transaction, in-transaction, and post-transaction phases, and should rely on objective indicators that are measurable, comparable, and verifiable.

One of the distinguishing features of the standard is its recognition that evaluation can be conducted internally by platforms (self-evaluation) or through external third-party assessments. In both cases, indicators play a central role as they provide a consistent basis for measuring efficiency, quality, and reliability of transaction services. The use of indicators allows stakeholders to assess performance on common grounds, communicate results clearly, and understand risks and bottlenecks from a shared perspective. In addition, this approach strengthens trust by making assurance visible and evidence-based.

Figure 2-4 ISO32112:2025 Relevant Factors of Evaluation and Selection of Indicators



Source ISO 32112 (2025)

10 This sub-section explains the contents of ISO 32112:2025. <https://www.iso.org/standard/81357.html?browse=tc>

4 Factors of evaluation for e-commerce transaction

ISO 32112 structures the evaluation process around four overarching factors, which are further divided into eighteen thematic areas. These factors reflect the multidimensional nature of transaction assurance and acknowledge that trust in e-commerce depends not only on platform performance but also on external environments and long-term sustainability.

- ① (5.2) Quality of e-commerce transaction platforms and sites
- ② (5.3) Quality of e-commerce transaction services
- ③ (5.4) Local external environments for the e-commerce transaction
- ④ (5.5) Sustainability of e-commerce transactions

Figure 2-5 4 Factors and 18 Themes of Evaluation for e-commerce Transaction



Source ISO 32112 (2025) p.5

The first factor is the quality of e-commerce platforms and sites. This includes technological capacity, interface design, information security, regulatory compliance, and brand trust or reputation. The standard evaluates whether platforms are capable of processing large transaction volumes, maintaining stable and error-free services, protecting data integrity, providing accessible and authentic user interfaces, and demonstrating transparent business practices. Security and compliance are viewed as integrated aspects of platform quality rather than isolated technical functions.

The second factor concerns the quality of e-commerce transaction services. This factor spans service provision across all transaction stages, including pre-sale interactions, order processing, payment execution, logistics operations, after-sales services, and other auxiliary services such as customer support and training. Evaluation focuses on responsiveness, accuracy of order information, payment traceability, delivery efficiency, return and refund mechanisms, and the ability to resolve disputes or compensate users. The standard stresses the need for seamless connections between these services, meaning that failure in one area—such as delivery or after-sales support—can undermine the credibility of the entire transaction process.

The third factor addresses the external environment in which e-commerce operates. This includes the broader business climate, government initiatives and support mechanisms, supervision frameworks, and access to finance for e-commerce actors. ISO 32112 acknowledges that even well-designed platforms may struggle to ensure transaction assurance in an unsupportive regulatory environment or where infrastructure gaps exist. Therefore, the evaluation considers whether external environments facilitate collaboration between stakeholders, provide fair oversight, offer incentives for innovation, and ensure access to financial resources for start-ups and SMEs.

The fourth factor relates to the sustainability of e-commerce transactions. Sustainability is evaluated across economic, social, and environmental dimensions. Economic sustainability involves the use of emerging technologies, innovation models such as social commerce and live-streaming, and resilience against supply chain disruptions. Social sustainability focuses on inclusiveness, such as enabling rural participation, supporting SMEs, or improving accessibility for elderly or disabled users. Environmental sustainability evaluates whether platforms adopt green practices, reduce waste through reverse logistics, promote renewable energy, and contribute to carbon footprint reduction. Sustainability is not treated as a secondary concern but as an integral component of long-term trust in e-commerce.

Use of Indicators

To operationalize these four factors, ISO 32112 promotes the use of measurable indicators. Indicators act as reference points to evaluate performance, benchmark progress, communicate results transparently, and detect weaknesses within transaction

activities. They may include quantitative metrics—such as average payment failure rate, delivery lead time, refund processing time, server downtime, number of cyber incidents—or qualitative assessments such as user satisfaction, accessibility for vulnerable groups, or clarity of terms and conditions.

The standard provides a catalogue of example indicators across all eighteen themes—such as platform processing capacity, user interface accessibility, order accuracy, logistics traceability, financial inclusiveness, regulatory oversight, and environmental impact. These are not mandatory but serve as reference options that can be adapted to national contexts or platform-specific needs. In the context of Ethiopia, such indicators could serve as the foundation for future certification schemes aligned with the Electronic Transactions Proclamation, the Digital Consumer Protection Directive, and the Personal Data Protection Proclamation.

Quality of e-commerce transaction platforms and sites

► Processing Capacity

E-commerce transaction platforms and sites should have processing capacity that is: — functional, which means, being able to ensure smooth functioning of foundational E-commerce features, including account registration and sign-up processes, searching on websites and mobile applications specifically designed for sellers; — customizable, which means, offering flexible solutions that can expand to accommodate increased demand and providing alternative options to suit buyers' personal preferences, including product search functionality for e-shops/e-stores. It is crucial to ensure that buyers are not tracked without their knowledge. Safeguarding buyers' personal registered information and privacy is of paramount importance; — responsive and dynamic, which means, being equipped with the ability to adapt and react effectively, which includes timely releasing of transaction-related information, verification of registered information, prompt response to requests, capacity of maintaining low latency, redundancy and failover, timely updated search functions, and a convenient verification and approval process; — stable and error-free, which means, being capable of handling a high-frequency trading volume while offering functions such as ease of maintenance and technical support, quick recovery, cache efficiency, load balancing effectiveness, etc.

► Interface

E-commerce transaction platforms and sites should have interfaces that are: — authentic and validated, which means, being able to provide valid and accurate information or feedback and transaction progress information to users, visitors, or third parties associated with an E-commerce platform; — user-friendly, which means, being designed for easy navigation that enables users to be easily directed to the sellers' entries, online dispute resolution (ODR), maintenance and technical support, searching

functionality, user onboarding, and ensuring a consistent clarity in design, typography, readability and multilingual support; — regularly assessed and maintained, which means, being capable of carrying out quality assessment through client feedback, performance monitoring, and secure testing

► Information security and management measures

E-commerce transaction platforms and sites should have information security and management measures that are: — well-protected, which means, being capable of ensuring safety and security for transaction databases by means of utilizing transaction databases in a legal and secure manner, physical security measures, database backup-restore, permissions or access control, etc.; — confidential, which means, ensuring the prevention of transaction related-information leakage throughout the entire process of E-commerce transactions to protect user privacy; — integral, which means, being capable of ensuring that all necessary transaction details are stored and accurate; — effective and robust, which means, providing operational support, such as timely processing, reliable tracing and permissions or hierarchical access control for transaction-related information.

► Compliance

E-commerce transaction platforms and sites should have compliance measures that are: — integrated and information consolidated, which means, being outfitted with all necessary information, including terms and conditions, software, resolving disputes, connectivity, contact information, and preparation of third-party services; — transparent and verifiable, which means, capable of being open to the public and easily accessible for query, browsing, and future retrieval well-connected and easily available, which means, being designed for a clear, measurable and understandable platform, helping various sellers or buyers to handle transactions efficiently; — compatible, which means, being able to ensure that an E-commerce transaction platform complies with all relevant statutory and regulatory requirements in the jurisdictions where the transaction occurs locally; — reliable, which means, being incorporated with intellectual property protection measures to promptly address any potential intellectual property rights (IPR) infringements

► Trust and brand reputation

E-commerce transaction platforms and sites should cultivate trust and brand reputation that is: — objective and accurate, which means, being able to assure the true and valid provision of information, such as product descriptions, credit of e-shops/e-stores and reviews by buyers; — fair, which means, being able to ensure that everyone has equal opportunities to participate in the E-commerce transactions. For example, the reviews of the E-commerce platforms and sites should be accessible to everyone, ensuring equal

access for small and medium-sized enterprises, and offering assistance to individuals with disabilities who wish to participate in transactions; — promptly responding, which means, being capable of addressing issues such as fraudulent behaviours in a timely manner; — immutable and discoverable, which means, being able to ensure publicly available information related to the E-commerce transactions, such as brand information, logistic information, reviews, and assessment information of e-shops/e-stores, etc., is easy to access and understand. Additionally, any changes made to this information should be transparent and clearly visible to all.

Table 2-5 Example Indicators : Quality of e-commerce transaction platforms and sites

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.2.1 Processing Capacity	Functional	Page load time, mobile responsiveness	Avg. page load time (sec), % of failed webpage loads	Platform Operator, Ethio Telecom
	Customizable	% of customers using personalized options	% of SMEs using local-language UI/ custom features	Platform + MinT (Digital Inclusion Directorate)
	Responsive & dynamic	Avg. time to resolve system failures	Time to restore service after failure; system latency	INSA (Information Network Security Admin) + Platforms
	Stable and error-free	Error rate, peak load capacity	System uptime (%), number of crashes per month	Platform Operator, INSA
5.2.2 Interface	Authentic & validated	% of verified sellers/products	% of e-marketplace sellers with business license/TIN verified	MinT + Ethiopian Revenues & Customs Authority (ERCA)
	User-friendly	Number of steps to reach customer service	Avg. number of clicks to reach help/ complaint page	Platform UX Team + Ethiopian Consumer Protection Authority
	Regularly assessed & maintained	% of issues identified through UX testing	Number of platform updates based on user feedback	Platforms

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.2.3 Info Security	Well-protected	Number of unauthorized data access incidents	Number of cyber incidents reported per year	INSA (Cybersecurity) + Platforms
	Confidential	Number of data leak incidents	% of encrypted personal/payment data	Platforms + Data Protection Commission (under Proclamation 1321/2024)
	Integral	% of accurately stored transaction data	% of transactions with tamper-proof logs	Platforms + National Digital ID Program
	Effective & robust	Compliance with access-control policies	% of staff trained in cybersecurity annually	Platforms + INSA
5.2.4 Compliance	Integrated & info consolidated	% of transactions where all information is accurately provided	% of platform listings displaying price, tax, seller info clearly	MinT (licensing), Trade & Consumer Protection Authority
	Transparent & verifiable	% of publicly available transaction info	Number of platforms publishing transparency reports	MinT
	Well-connected & available	No major performance degradation	System uptime during peak demand (ex. Black Friday, Meskel Holiday Sales)	Platforms
	Compatible	Frequency of platform updates to match regulation	Average time to implement new legal requirements (e.g., VAT, data privacy)	MinT + ERCA
	Reliable	No. of infringement complaints resolved	% of customer complaints resolved within 15 days	Consumer Protection Authority

Source ISO 32112 (2025)

Quality of E-commerce transaction services

► Pre-sale services

The quality of pre-sale services in E-commerce transactions should be evaluated in terms of: — various contact options available, which means, being equipped with a variety of channels, including online, telephone, and personalized consulting services, as well as multi-language support, empowered customer service representatives, and integration of artificial intelligence (AI) systems and chatbots, that efficiently handle any inquiries or concerns related to pre-sales customer services; — quick and agile, which means, being capable of prioritizing responses to enquiries and time commitments; — streamlined and accessible, which means, being equipped with multiple channels for obtaining comprehensive product information and lodging complaints, by means of interactive and real-time live room influencer responses, phone, email, online and human or AI-powered customer services, which are easily accessible and efficiently handled; — well-established, which means, being designed for the placement of electronic orders, incorporation of order tracking, record-keeping, and customer relationship management (CRM) integration to cater to buyers who demand further consultation or confirmation of electronic orders.

► Order services

The quality of order services in E-commerce transactions should be evaluated in terms of: — timely updated, which means, being capable of ensuring the accuracy and completeness of transaction related information, including descriptions, delivery dates, precise and holistic real-time order tracking, and notices communicable and reachable, which means, being assured of smooth communication between the sellers and buyers, such as real-time interaction between influencers and buyers in live streaming studios; — interoperable, which means, being designed to ensure seamless and timely processing of orders, such as automatic order confirmation emails, real-time inventory management, mobile-compatible guest checkout options, and fast delivery options, especially for cross-border transactions, up-to-date currency exchanges, custom duties and confirmations of the electronic order. They should also be compatible with pre-sales services and after-sales services; — transaction records documented, which means, assuring that confirmation of electronic orders are safely stored for a specified retention period for accountability and future reference. Additionally, they should provide order history and account integration.

► Payment services

The quality of payment services in E-commerce transactions should be evaluated for: — multiple options available, which means, being able to offer a choice of payment methods for products, such as cash on delivery, online payment, post office remittance,

e-banking, and credit cards, etc; — countable and proactive, which means, being capable of promptly and effectively addressing any queries, ensuring the traceability of payment information in transactions; — secured and safe, which means, being able to ensure payment information is used and interconnected safely between platforms, sellers, buyers, logistics, and other recipients; — adaptive and resilient, which means, being equipped to manage transaction risks, payment failures, and frauds against transactions and payments, and to implement measures such as payment verification, instant notification, and reconfirmation to prevent and mitigate issues.

► Logistic services

The quality of logistics services in E-commerce transactions should be evaluated for: — complete and extensive, which means, being able to offer account management, delivery of purchased products, inventory management, innovative warehousing management, and customs clearance to support logistics for all transactions; — traceable and queryable, which means, being able to track the entire logistics process from dispatch, distribution, and last-mile delivery of purchased products to the final consumer. Real-time tracking and SMS or email notifications can enhance the customer experience; — confidential, which means, being able to ensure that the logistics details match between sellers and E-commerce platforms whilst protecting the privacy and data security of related participants; — tailor-made, which means, outfitting with personalized logistics options such as custom packaging, specialized transport, vendor-managed inventory, urban distribution, door-to-door pickup, and other last-mile delivery solutions; — reversed, which means, being able to offer a reverse logistics system that can manage the return, repair, recycling, or disposal of goods from their final destination to a resource hub, maximizing the value recovery from returns while minimizing waste and environmental impact.

► After-sales services

The quality of after-sales services in E-commerce transactions should be evaluated for: — flexible and selective, which means, providing multiple hassle-free and flexible product return or replacement options, such as no-reason-required replacements, trial periods for returns, and a range of alternatives for replacement; — efficient and refundable, which means, being equipped with various refund options, such as refunds according to contract or agreed rules, and customer retention offers. An E-commerce customer service representative can determine open refund cases; — customer-centric, which means, addressing complaints and reviews from buyers, being accessible to various unbiased dispute resolution mechanisms, and being provided with feedback to improve customer satisfaction; — reasonable and insured, which means, being able to offer a variety of compensation for transaction loss and insurance options, including clear guidelines on

claims, margin compensation, exemptions, compensation standards, and coverage; — straightforward and evident, which means, being outfitted with prompt and genial service responses, and clearly defined terms that are easily understood; — interactive, which means, being capable of facilitating real-time engagement between sellers and buyers with features such as live Q&A sessions, product demonstrations, and instant feedback mechanisms to enhance the shopping experience.

► Miscellaneous services

Miscellaneous services in E-commerce transactions can be evaluated for: — clear and useful, which means, being able to provide guidance or courses for opening and operating e-shops/e-stores, such as seller success stories or case studies, as well as performance analytics and insights; — skilled and capacity-enabled, which means, being capable of refining communication and presentation skills, having an in-depth understanding of products, enhancing interactive abilities and demonstrating technical proficiency by influencers in live streaming studios. It also means establishing a comprehensive training system that includes pre-job training, on-the-job training, skills training, seminars, digital marketing workshops, and vendor education programs; — specialized, which means being able to provide professional support teams in live commerce, such as operating multi-channel networks (MCNs), excelling in product selection, possessing adept video production skills, and managing technical setups involving equipment, lighting, and audio adjustments in live commerce; — marketing-enabled, which means, being able to offer various marketing approaches, such as E-commerce shopping festivals, promotions, pop-up advertisements, localized marketing campaigns, and digital and offline promotional events for brands.

Table 2-6 Example Indicators: Quality of E-commerce Transaction Services

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.3.1 Pre-sale Services	Various contact options	No. of available complaint/contact channels	No. of functional contact channels (call center, email, chatbot, Amharic/ local language support)	Platforms, MinT
	Quick & agile	Avg. response time to inquiries	Avg. customer response time (seconds/hours)	Platforms
	Streamlined & accessible	Clarity of pricing and terms	% of product pages showing full price (incl. VAT, delivery)	Platforms, ERCA (Tax Authority)

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.3.1 Pre-sale Services	Well-established	Order placement & CRM integration	Availability of order tracking before payment	Platforms
5.3.2 Order Services	Timely updated	Order fulfilment rate	% of orders processed within promised time (i.e. 48 hrs, 7 days, etc.)	Platforms Ethiopian Postal Service (or other logistics providers)
	Communicable & reachable	Communication coverage	% of customers able to contact seller in real-time	Platforms
	Interoperable	Real-time tracking, inventory sync	Existence of e-invoice + digital order confirmation	Platforms, MoTRI
	Records documented	Length of record retention	Minimum 2-year digital record retention of orders (aligned with ISO/ET law)	Platforms, MinT
5.3.3 Payment Services	Multiple options	No. of available payment methods	Cash on delivery %, mobile money %, digital wallet usage	National Bank of Ethiopia (NBE), Platforms
	Countable & proactive	Avg. response time to payment queries	% of disputed payments resolved within 7 days	NBE, Platforms
	Secure & safe	No. of payment data breaches	Payment fraud cases reported annually	NBE, INSA
	Adaptive & resilient	Ability to handle payment risk	Payment system uptime during Cyber Week/Meskel Holiday	Platforms, NBE
5.3.4 Logistics	Complete & extensive	No. of functions: tracking, warehousing	% of deliveries with end-to-end tracking	Ethiopian Postal Service, Ride Logistics, etc.
	Traceable & queryable	Tracking update frequency	Avg. number of tracking status updates per delivery	Platforms, Logistics providers
	Confidential	Security & privacy in logistics	% of deliveries where personal info is encrypted	Logistics providers, INSA

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.3.4 Logistics	Tailor-made	Custom logistics	% of SMEs using customized delivery (door-to-door, pickup stations)	Logistics providers
	Reversed (Return logistics)	Reverse logistics rate	% of products returned and successfully collected	Platforms Logistics providers
5.3.5 After-sales	Flexible & selective	No. of return/ replacement options	% of categories offering “no-reason return”	Platforms, MinT
	Efficient & refundable	Refund processing time	Avg. number of days to issue refund	Platforms
	Customer-centric	Complaints handled	% of complaints resolved within legal period (i.e. 15 days)	Ethiopian Consumer Protection Authority
	Reasonable & insured	Return insurance coverage	% of transactions covered by delivery insurance	Logistics providers, Insurance Companies
	Interactive	Instant feedback rate	Avg. response time to post-purchase inquiry	Platforms
5.3.6 Miscellaneous	Clear & useful	No. of e-shop guides/training	No. of vendors trained on digital sales by MinT	MinT, relevant education agencies
	Skilled & capacity-enabled	% of staff trained	% of platform employees completing annual e-commerce training	Platforms
	Specialized (Live Commerce)	Live engagement rate	Avg. live-stream viewers/ transactions per session	Platforms + Influencer Networks (MCNs)
	Marketing-enabled	Customer acquisition cost	Cost to acquire 1 new customer	Platforms

Source ISO 32112 (2025)

Local external environments for E-commerce transactions

► Business environment

The local external business environment for E-commerce transactions should be evaluated for: — collaborative and credible, which means, being able to involve different interested parties in order to exchange information. For example, organizing associations or events to exchange industry information, including transaction policies and technology trends— adaptable, which means, being able to adapt to various changes, such as providing training on new technologies, or adjusting the management approach to respond to the changing industry trends; — resilient, which means, being capable of responding and recovering from crises such as public health emergencies, through measures including rebuilding trust and coordinating supply chains.

► Initiatives and measures

Local initiatives and measures for E-commerce transactions should be evaluated regarding for: — incentivized, which means, being equipped with incentive measures to encourage more participants to engage in the E-commerce industry; — instructive and facilitative, being designed to create initiatives that promote the growth of cross-border E-commerce and facilitate investment in E-commerce transaction infrastructure; — impartial and protective, which means, being outfitted with relevant measures to encourage the involvement of start-ups and small- and medium-sized participants in E-commerce transactions.

► Supervision

Supervision from local external environments for E-commerce transactions should be evaluated for: — multifaceted and polycentric, which means, being outfitted with government surveillance, neutral party supervision, or media supervision; — equitable, which means, being equipped with supervision to ensure that all concerns from sellers and buyers can be addressed in a fair and transparent communication environment; — swift, which means, being able to ensure that entities being supervised respond swiftly to address concerns and outcomes of E-commerce transactions in a timely manner.

► Availability of financing

Availability of financing in local external environments for E-commerce transactions should be evaluated for: — easily obtainable, which means, offering financing opportunities for small and medium-sized enterprises, including credit, guarantees, financial leases, bonds, insurance, funds, and investments from internal or external sources; — proactive, which means, being able to offer active and professional financing assistance to ensure that they remain aligned with their business objectives.

Table 2-7 Example Indicators: Local external environments for E-commerce transactions

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.4.1 Business environment	Collaborative & credible	No. of participants in industry associations/ exchange events	No. of active e-commerce associations (e.g. Chamber of Commerce, ICT Associations)	MinT, Ethiopian Chamber of Commerce, Private Sector
	Adaptable	Avg. time to respond to market changes	Time required to update digital commerce regulations (e.g. VAT, data protection)	MinT, MOF (Ministry of Finance)
	Resilient	% of customer confidence regained post-crisis	Restoration time of e-commerce platforms after internet shutdown/ COVID-19-like disruption	Ethio Telecom, INSA, MinT
5.4.2 Initiatives & measures	Incentivized	% of businesses covered by incentive policies	Number of SMEs receiving tax incentives/logistics subsidies for e-commerce	MOF, MinT
	Instructive & facilitative	% of cross-border e-commerce supported by policy	Number of government programs promoting cross-border trade (e.g. AfCFTA Digital Protocol)	Ethiopian Customs Commission , MoTRI, MinT
	Impartial & protective	No. of policies for vulnerable groups	Number of measures introduced to support women-owned, youth-owned, or rural e-commerce businesses	MinT, Ministry of Women & Social Affairs
5.4.3 Supervision	Multifaceted & polycentric	No. of supervisory audits per year	Number of inspections by MinT, Consumer Protection Authority, Data Protection Office	MinT, Trade Competition & Consumer Protection Authority (TCCPA)

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.4.3 Supervision	Equitable	% of buyers satisfied with supervision fairness	Consumer satisfaction index for e-commerce dispute handling	TCCPA
	Swift	% of feedback resolved within 48 hours	Avg. time for regulators to act on consumer complaints	MinT, Consumer Protection Authority
5.4.4 Financing availability	Easily obtainable	% of successful financing access for SMEs	Number of start-ups receiving e-commerce financing / grants / microcredit	NBE, Ethiopian Enterprise Development (EED)
	Proactive	% of businesses receiving digital transformation funding	Number of fintech/ e-commerce firms receiving risk capital or innovation grants	NBE, MinT, Private banks

Source ISO 32112 (2025)

Sustainability of E-commerce transactions

► Sustainability in economy

Sustainability in economy related to E-commerce transactions should be evaluated for: — new-norm empowered, which means, adopting cutting-edge technologies, such as unmanned storage facilities, mobile payments, digital wallets, blockchain-based solutions, non-contact services, unmanned delivery, or artificial intelligence (AI) systems, to improve the buyer experience, increase business efficiency, and reduce costs; — innovative, which means, being capable of adopting practices like livestreaming, social commerce, and group buying to enhance the buyer's experience and improve transaction volume; — inclusive, which means, being able to encourage equal opportunities in innovation and entrepreneurship for everyone, which can improve inclusiveness resource-efficient and resilient, which means, ensuring that the processes along the E-commerce supply chains are resource-conscious, including sustainable procurement, selecting sustainable manufacturers, and sustainable sales.

► Sustainability in society

Sustainability in society related to E-commerce transactions should be evaluated for: — engaging and supportive, which means, being capable of empowering multiple sellers, including small and medium-sized enterprises and isolated countryside sellers,

to increase employment rate and promote product sales in small and medium-sized cities and rural areas; — diversified and productive, which means, being designed to increase cross-border exchange opportunities, to provide more interaction methods for cross-border sellers to interact by using social E-commerce platforms, for example, and to improve the diversity of product sales and interactions between sellers and buyers; — cost-effective and convenient, which means, capable of providing more convenient options that help to alleviate poverty and enable human beings living in far areas or with mobility issues to purchase goods easily.

► Sustainability in environment

Sustainability in environment related to E-commerce transactions should be evaluated for: — environment-friendly, which means, adopting sustainable practices such as reducing products' carbon footprint, using renewable energy sources, minimizing pollution emissions, offering net-zero carbon labels, publishing ESG reports and reducing the usage of harmful chemicals and pollutants; — reduced, reused and recycled (3R) adopted, which means, encouraging the recycling of packaging materials, reusing electronic devices, reducing waste through reverse logistics, and reducing energy consumption through sustainable practices.

Table 2-8 Example Indicators: Sustainability of E-commerce Transactions

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.5.1 Economic sustainability	New-norm empowered	No. of new payment or digital tools per year	Number of new digital payment tools launched (i.e.: TeleBirr, HelloCash, M-Pesa, etc.)	NBE, Fintech firms
	Innovative	Customer satisfaction with new practices	% of SMEs adopting live commerce, AI chatbots, social commerce	MinT, Private Platforms
	Inclusive	Participation across categories	% of women/youth-owned SMEs on platforms (Jumia, Zmall, etc.)	Ministry of Women & Social Affairs, MinT
	Resource-efficient & resilient	% of sustainably sourced products	% of platforms using cloud services, renewable-powered data centers	Ethiopian Electricity Utility, Private Data Centers

Theme	Consideration Point	ISO Example Indicator	Application in Ethiopia: Possible Indicators	Responsible Authority in Ethiopia
5.5.2 Social sustainability	Engaging & supportive	Job growth from e-commerce	No. of jobs created via e-commerce platforms (couriers, sellers, influencers)	Ministry of Labor & Skills
	Diversified & productive	% of cross-border sales in e-commerce	Volume of e-commerce exports via AfCFTA Digital Trade	Ethiopian Customs Commission, MinT
	Cost-effective & convenient	Avg. price comparison (platform vs local markets)	% price difference of key goods between e-commerce and physical markets	Trade Competition & Consumer Protection Authority (TCCPA)
5.5.3 Environmental sustainability	Environment-friendly	Carbon footprint reduction rate	% of logistics fleet using electric/renewable fuel vehicles	Ministry of Transport & Logistics, Green Legacy Initiative
	Reduced / Reused / Recycled (3R)	Reuse of devices, waste reduction rate	% of recyclable packaging in e-commerce deliveries	Ministry of Environment, Forest and Climate Change
	Reverse logistics	Reverse logistics efficiency	% of returned goods recycled, resold, or refurbished	Platforms, Postal/ Logistics providers

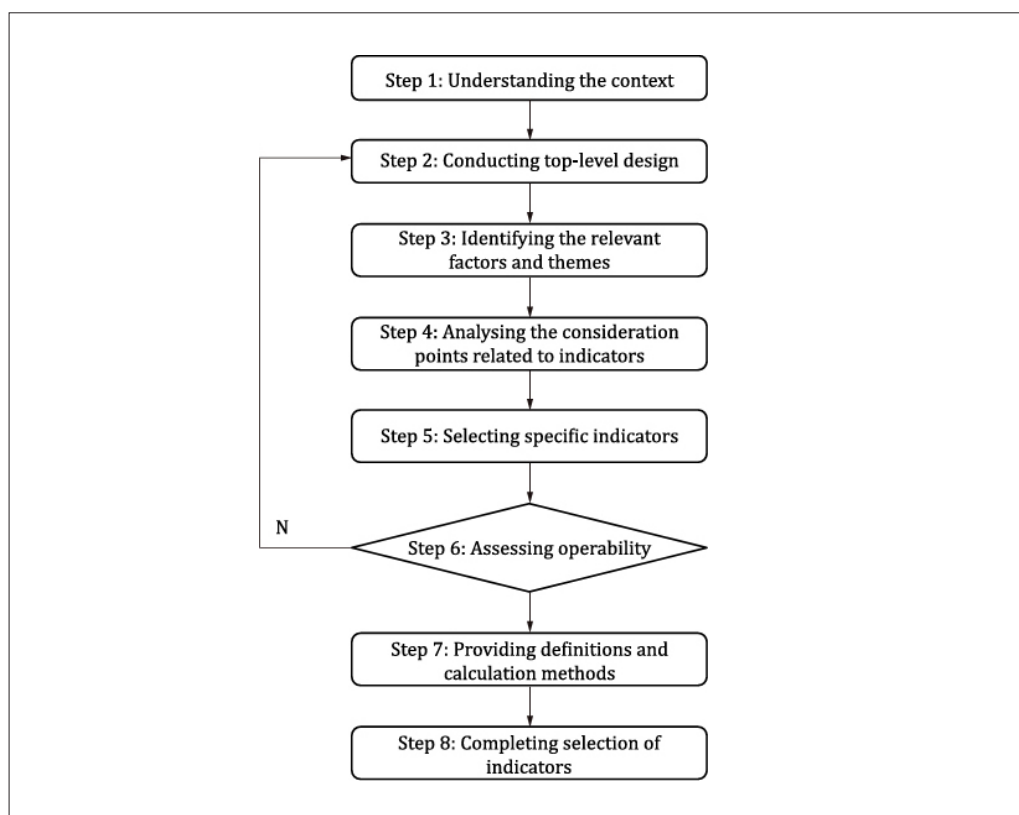
Source ISO 32112 (2025) p. 17

Selection of indicators

The selection of indicators follows a systematic process that begins with understanding the context and defining a high-level design. Relevant factors and themes are then identified, followed by an analysis of the consideration points and the selection of appropriate indicators. Each indicator is assessed for operability, and only those that can be practically measured are retained. The final step involves clearly defining each indicator and its calculation method.

Indicators are essential because they make the performance of e-commerce transactions measurable. They provide quantifiable and comparable results, help assess quality and efficiency, reveal problems and bottlenecks, and support a common understanding among stakeholders. By doing so, indicators strengthen transparency, security and trust in the e-commerce environment.

Figure 2-6 Procedures to Select Appropriate Indicators



Source ISO 32112 (2025) p. 13

2.3. Case Studies : ROK e-Trust Mark Certification System (1999–2017)

The Republic of Korea introduced the eTrust Certification System in 1999 as one of the earliest government-supported initiatives to enhance confidence in online commercial transactions. The certification was designed to be granted to e-commerce operators that demonstrated excellence in consumer protection, privacy management, online security, and overall transaction reliability. Its core objective was to build trust in digital transactions by assuring consumers that certified websites complied with recognized standards of safety, transparency, and fair business practices.

The legal foundation for the system was provided by Article 18 of the Framework Act on Electronic Transactions,¹¹ which states that the government may support certification programs for outstanding e-commerce businesses to protect consumers and promote the

sound development of digital markets (Annex 1). The program primarily targeted online shopping malls that had been in operation for at least three months and assessed the entire transaction process—from pre-contractual information and ordering to payment, delivery, return policies, and post-sale services. Certification was valid for one year and renewal required an additional evaluation and payment of fees scaled to the business size.

Table 2-9 ROK eTrust Certification System : Legal Background

Framework Act on Electronic Documents and Transactions (ROK)	
Article 18 (Certification of Electric Transaction Business Entities)	(1) The Minister of Science, ICT and Future Planning may certify an exemplary electric transaction business entity in order to promote electronic transactions and protect electronic transaction users. (2) The Minister of Science, ICT and Future Planning may collect fees from a person who files for certification under paragraph (1). (3) Standards and procedures for certification under paragraph (1) and fees collected under paragraph (2) and other necessary matters shall be prescribed by Presidential Decree.
Article 22 (Agency Exclusively Responsible for Promoting Use of Electronic Documents and Conduct of Electronic Transactions)	(1) The Ministry of Science, Information and Communications Technology (ICT) and Future Planning may designate an exclusively responsible agency to implement the following projects in an efficient and systematic manner for facilitating the use of electronic documents as well as the conduct of electronic transactions: 1. Support for certification of facilities or equipment creating digitized documents under Article 23 (3); 2. Research and development and dissemination projects of standards related to electronic documents and electronic transactions under Article 24, and activities related to the international standardization of such standards; 3. Support for technical development under Article 25; 4. Support for fact-finding surveys of statistics on electronic documents and electronic transactions under Article 28; 5. Support for duties of designating certified electronic document centers under Article 31-2; 6. Support for reporting of working rules, such as the storage of electronic documents, under Article 31-8; 7. Support for technologies on measures for protecting electronic documents by certified electronic document centers under Article 31-9 (3); 8. Acquiring stored documents, etc. under Article 31-15 (3); 9. Support for duties of designating certified electronic documents intermediaries under Article 31-18; 10. Operation of the Mediation Committee of Disputes on Electronic Documents and Transactions under Article 32.

Source ROK Framework Act on Electronic Documents and Transactions (2016)

¹¹ FRAMEWORK ACT ON ELECTRONIC DOCUMENTS AND TRANSACTIONS (Revision 2016., not current)
<https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=179518&chrClsCd=010203&urlMode=engLsInfoR&viewCls=engLsInfoR#EJ18:0>

Table 2-10 ROK eTrust Certification System: Operating Agency

Period	Operating Agencies
1999–2009	Operating Institution: Korea Institute for Electronic Commerce (KIEC), Dong-A Ilbo, Korea Economic Daily, Digital Times Supporters: Ministry of Knowledge Economy, Association of eTrust-Certified Companies
2010–2015	Operating Institution: National IT Industry Promotion Agency (NIPA)* NIPA operate “Electronic Transaction Dispute Mediation Committee”

Source Digital Daily (July 1, 2010)¹² Kyung Hyang News (August 30, 2001)¹³

The evaluation criteria of the eTrust system reflected a comprehensive understanding of transaction assurance. Assessment areas included website usability and safety, transparency of business and product information, ordering and payment procedures, delivery, return and refund processes, system and data security, personal information protection, compliance with consumer protection laws, and the quality of post-sale customer service. Certification covered different industry sectors, including general and specialty shopping malls, finance, trade, travel, leisure, B2B platforms, and brokerage services, with tailored criteria for each category.

Table 2-11 eTrust Certification System Outline

Category	Description
Target	Online shopping malls that have been in operation for more than three months
Scope of Certification	Entire e-commerce transaction process and appropriateness of the business model
Validity Period	Certificate valid for 1 year; annual fee applied based on business size and duration of certification
Post-Certification Monitoring	eTrust Cyber Support Team conducts regular monitoring of certified companies to ensure continued compliance with certification criteria and addresses consumer complaints or operational issues
Evaluation Criteria	
Website usability and safety	Evaluation of user experience, navigation, accessibility, and secure access
Transaction process	Includes ordering procedures, payment systems, and transaction flow
Delivery, exchange, and return policies	Assessment of delivery reliability, return/refund procedures, and consumer rights protection

• Transparency of corporate and product information	Accuracy and completeness of company identity, product descriptions, pricing, and terms
• System security	Assessment of security measures, encryption, data storage, and cyber risk management
• Personal data protection	Compliance with privacy policies, data handling practices, and user consent mechanisms
• Post-sale customer support	Availability and quality of after-sales service, complaint handling, and dispute resolution
• Legal compliance	Adherence to e-commerce consumer protection laws and relevant regulations

Source NIPA (2012)

The certification process involved application submission, documentation review, on-site or remote evaluation of website operations, corrective feedback, a final decision by a review panel, and the issuance of the eTrust mark. Certified companies were required to display a standardized eTrust certification page on their websites, enabling consumers to verify the authenticity of the certification and review key corporate information. After certification, NIPA conducted regular monitoring through the “eTrust Cyber Support Team” to confirm continued compliance and identify areas for improvement.¹⁴

Beyond certification, the program provided additional support to small and medium-sized enterprises (SMEs). Certified businesses received priority handling in dispute mediation, access to consulting services to improve website compliance, inclusion in a dedicated section of the Korea Post online marketplace, lower commission fees, and one-on-one product consulting. The eTrust Certified Business Association also facilitated peer collaboration and collective marketing.

¹² <https://m.ddaily.co.kr/page/view/2010070115344780279>; https://www.kocca.kr/knowledge/research/__icsFiles/afieldfile/2012/01/20/ZVY0mlvxupPh.pdf

¹³ <https://www.khan.co.kr/article/200108301317321>

¹⁴ <https://www.nipa.kr/home/2-1/10588>
https://www.kocca.kr/knowledge/research/__icsFiles/afieldfile/2012/01/20/ZVY0mlvxupPh.pdf

Table 2-12 Evaluation Criteria

Area/Sector	Criteria	Area/Sector	Criteria
Common Area	Business Information, Safety, Privacy Policy and Terms, Payment System, Post-Sale Customer Service	Finance Sector	Transaction Information, Market Information, Transaction Process, Customer Support
Shopping Mall Sector (General / Specialized / D2C)	Product Information, Order Process, Delivery Process, Customer Service	Trade Sector	Contract Management, Logistics & Finance, Offer, Product Catalog, Member Support
Travel & Leisure Sector	Product Information, Order Process, Delivery Process, Customer Service	B2B Sector	Product Information, Purchase Process, Sales Process, Payment Request, Delivery Handling, Customer Support
Brokerage Section	Item Information, Auction Process, Delivery Process, Customer Support	Service Sector	Product Information, Service Delivery Process, Customer Support

Source NIPA

Evidence shows that the certification system contributed positively to consumer trust and market stability. As of 2010, only 120 out of 3,200 dispute mediation applications (3.8 percent) involved eTrust-certified businesses, and the dispute resolution rate reached 96 percent. Certified companies accounted for over half of national online sales, demonstrating both the credibility and economic influence of the certification scheme. Furthermore, cooperation with international organizations such as the Global Trustmark Alliance (GTA) and Asia Trustmark Alliance (ATA) supported overseas market entry for Korean firms.

Nevertheless, by the mid-2010s, new challenges emerged. Consumers increasingly relied on user reviews, comments, and social media rather than certification logos to determine platform reliability. Some critics also noted that government support for certified businesses weakened over time in areas such as export promotion and international marketing. Meanwhile, the rising number of complaints related to fraud, delayed delivery, refusal of refunds, and misuse of consumer data indicated that certification alone could not fully address trust deficits in a rapidly evolving digital economy.

Despite these limitations, the eTrust system played a pioneering role in institutionalizing transaction assurance and provided Korea with a structured model for platform evaluation, dispute management, and international cooperation in trustmark governance. Its experiences offer practical lessons for developing countries seeking to

design trustmark systems that support consumer protection, SME competitiveness, and cross-border digital trade.

2.4. e-Commerce Trust in Ethiopia and Recent Development

Ethiopia, with its large domestic market, growing manufacturing industry, and strategic position, holds significant potential for expanding e-commerce within its local and broader continental markets. Ethiopia has demonstrated strong political commitment to digital transformation and e-commerce development. Several policy developments represent this momentum:

- “Proclamation to Provide for Electronic Transactions” (2020): Established the legal foundation for recognizing electronic contracts, signatures, and digital evidence in commercial activities.
- Draft “Digital Consumer Protection Directives” (2023–2024): Aims to strengthen consumer rights in digital transactions, ensuring fair treatment, transparency, and mechanisms for redress.
- E-Commerce as a strategic tool for exports: Ethiopia views digital trade as a new channel for youth entrepreneurship, SME participation, and cross-border market entry, particularly for creative goods, coffee, textiles, and tourism services.
- National e-Commerce Strategy (2024): Introduces specific goals on secure payments, logistics standards, digital identity, and certification systems for platforms.
- AfCFTA Digital Trade Protocol (2024): Provides a continental framework for digital trade, data governance, cybersecurity, and e-signatures—requiring member states like Ethiopia to align regulatory frameworks and standards.

2.4.1. National e-Commerce Strategy (2024): focus on trust, standards, and platform quality

Ethiopia's 2024 National e-Commerce Strategy places consumer trust at the center of market development and assigns concrete implementation tasks to key public agencies. Under Strategic Goal 2—“Increase consumer awareness, trust, and confidence in e-commerce”—the strategy calls for a standards-led approach to platform quality and a parallel push to adopt enabling technologies.

First, the strategy proposes the development of standards for e-commerce platforms based on international best practices. The Ministry of Innovation and Technology (MinT)

is tasked with issuing high-level guidelines for e-commerce enterprise architecture so that local platforms share a coherent strategic design, integrate systems more easily, and improve security. MinT is also directed to publish development principles that embed UI/UX and web-accessibility requirements—explicitly including considerations for persons with disabilities—so that trust is supported by usability as well as compliance. In parallel, the Information Network Security Administration (INSA) is asked to introduce an e-commerce certificate to verify a provider's legal existence and to set pre-business registration and licensing criteria that demonstrate competency in areas such as software development and security. Complementing these measures, the Ethiopian Communications Authority (ECA) is expected to release free usability and performance testing tools to help platforms diagnose bottlenecks and meet baseline service expectations.

Second, the strategy encourages the uptake of emerging technologies that can raise the quality and credibility of platforms. INSA is mandated to promote the use of best-practice quality and security standards—such as ISO 10008:2022 for business-to-consumer transactions—so that operators have practical references for fraud prevention and data protection. MinT, for its part, will promote the use of cloud platforms as a service to accelerate the development of robust, scalable e-commerce applications. Taken together, these actions link directly to the assurance logic set out in ISO 32111 and the measurement approach in ISO 32112: platforms should be built on transparent rules and auditable processes, and their performance should be trackable with objective indicators.

Figure 2-7 National e-Commerce Strategy: Goals related to e-Commerce Transaction Assurance

S2.2. Develop standards for e-Commerce platforms based on international best	
2.2.1 (MinT)	Develop high-level guidelines for e-Commerce enterprise architecture to provide strategic alignment, promote efficiency, ensure integration of systems, and improve the security of local e-commerce platforms
2.2.3 (MinT)	Develop e-commerce platform development principles that include UI/UX and web accessibility considerations for PWDs
2.2.5 (INSA)	Introduce an e-Commerce certificate for e-commerce providers to verify their legal existence and introduce pre-business registration and licensing criteria to confirm their competency to run an e-commerce business, e.g. software development, security
2.2.6 (ECA)	Develop and launch free usability and performance testing tools for e-Commerce platforms

Source National e-Commerce Strategy (2024)

2.4.2. Policy environment and near-term priorities

Drawing on recent external analyses (Mastercard Foundation, 2024; GSMA, 2024), Ethiopia's policy environment shows clear momentum toward market-building reforms, coupled with practical challenges that affect transaction assurance.

On the regulatory side, MinT is developing a regulatory sandbox dedicated to e-commerce. The sandbox will allow firms to test products and business models under supervisory oversight before full regulatory obligations apply, creating a safe pathway to iterate features such as payment flows, identity verification, and delivery models. In parallel, MinT is preparing a competency certification scheme for e-commerce providers. Beyond checking legal existence, the scheme is intended to surface organizational strengths and gaps—staff skills, security readiness, UI/UX maturity—and to signal baseline capability to consumers and investors. The Ministry of Revenue is finalizing an e-receipt platform that will issue electronic receipts and provide real-time interfaces for tax and trade authorities; once operational, this system should make transactions more traceable, lower disputes about proof of purchase, and facilitate refunds. The Strategy is also collaborating with Ethiopian Airlines to establish an e-commerce hub and fulfillment center to support cross-border sales across African markets; by reducing logistics frictions and providing shared infrastructure, the hub can help domestic sellers meet delivery-time expectations that underpin trust.

At the same time, several binding constraints remain. Many platforms, especially those in early growth stages, struggle with user acquisition and retention because marketing capacity is thin and working capital is limited. Some operators diversify into unrelated web services or rely on owner-led marketing, which rarely yields sustained traffic; the result is a cycle of low transactions and limited reinvestment. Consumer understanding of e-commerce processes is another friction: users may be unfamiliar with delivery timelines, shipping costs, and returns, and limited digital literacy makes it harder to complete payments or assess security cues on websites and apps. Trust deficits are visible in concerns over product quality, scams on social channels (for example, installment payments without delivery), and uncertainty about data privacy and security. These perceptions suppress demand even when platforms comply with rules.

Transaction enablers also present gaps. The absence—until the e-receipt system goes live—of universal electronic receipting reduces the ability of payment processors to authenticate and reconcile online sales, particularly where informal channels prevail. Refund practices are uneven, with no standardized procedures among merchants, buyers, and payment providers; this undermines confidence in dispute resolution and increases platform risk when escrow funds are released prematurely. Logistics performance varies, and last-mile reliability remains a differentiator rather than a norm.

2.4.3. Linking Current Developments to Transaction Assurance, Standards, and Trustmark Systems

Ethiopia's current policy direction provides a strong foundation for transaction assurance, yet it remains fragmented across individual reforms—such as the regulatory sandbox, competency certification, and e-receipt system. These initiatives, although valuable on their own, have not yet been systematized into a coherent national framework that can verify, signal, and certify trustworthiness in e-commerce transactions. This is precisely where internationally aligned standards (e.g., ISO 32111, ISO 32112) and a national e-commerce trustmark certification system could bring coherence and structure.

First, the government's plan to introduce competency certification for e-commerce platforms (MinT/INSA) indicates the beginning of a certification logic. However, the current approach focuses primarily on legal existence and operational readiness. To evolve into a transaction assurance certification system, this scheme would need to incorporate ISO-based assurance elements—such as identity verification, payment security, delivery reliability, consumer dispute handling, and data protection—and translate them into measurable compliance criteria.

Second, the development of an e-receipt system and the future establishment of an e-commerce hub with Ethiopian Airlines provide infrastructure for traceability and logistics integrity. Yet, without standardized procedures and third-party assurance processes, these systems alone cannot produce verifiable trust signals. Integrating these infrastructures into a national trustmark model—similar to Korea's eTrust Mark—would allow certified platforms to display a visible, government-recognized mark that assures consumers of platform reliability, secure transactions, and dispute resolution mechanisms.

Third, Ethiopia's regulatory sandbox can be leveraged not only as a space for innovation but as a testing ground for trustmark certification criteria. Platforms participating in the sandbox could pilot standardized UI/UX requirements, delivery service compliance, refund procedures, and consumer complaint mechanisms before full-scale certification. This approach mirrors global best practices, where trustmark systems evolve in parallel with standards-based evaluation models.

In this context, the next strategic step for Ethiopia is not merely to promote platform development but to establish a standardized, certifiable trust assurance framework, consisting of:

- ISO 32111-based principles and assurance elements, adapted to Ethiopian market realities;
- ISO 32112-based indicators to evaluate platform performance and readiness;
- A national trustmark or certification scheme that operationalizes these standards and provides a visible signal of compliance to consumers, investors, and international partners.

Such a system would create a closed loop of trust—from regulation (laws), to infrastructure (e-receipts, logistics hub), to standards (ISO-based guidelines), and finally to trust signaling (certification mark). This aligns Ethiopia not only with global best practices but also with its own national priorities of building trust, reducing disputes, and supporting SMEs in domestic and cross-border digital trade.

2.5. Policy Recommendations for e-Commerce Transaction Assurance in Ethiopia

2.5.1. Mapping of Assurance elements to e-Transaction Phases

The e-commerce transaction process comprises a series of interdependent activities that span the pre-transaction, in-transaction, and post-transaction phases. ISO 32111 structures these activities around corresponding assurance elements—such as identity verification, payment security, delivery assurance, and dispute resolution—which collectively ensure transparency, reliability, and accountability throughout the transaction lifecycle. To support Ethiopia's efforts to operationalize transaction assurance, these assurance elements were mapped against existing legal provisions, institutional mandates, and anticipated responsibilities under Ethiopia's evolving regulatory framework. The following tables illustrate how ISO 32111 assurance elements align with Ethiopia's current and emerging regulatory environment, identifying the relevant legal basis and responsible authority for each activity.

Table 2-13 Mapping the Assurance Elements : Pre-transaction Phases			
Activity (ISO 32111)	Assurance Element	Ethiopian Legal Basis	Responsible Authority
Account registration	Identity information (8.2); Qualification info (8.3); Product info (8.7)	Registration info set & MinT verification/ licensing (1-year) ; trade registration prerequisite	MinT (e-Commerce platfor registration); Relevant Authority (MoTRI: business registration)
Verification of registered info	Identity (8.2); Qualification (8.3)	Renewal: renewed trade registration + security compliance	MinT
Preparation of third-party service	Third-party service rule (8.5)	Cybersecurity assessment by recognized security agency	MinT, INSA

Activity (ISO 3211)	Assurance Element	Ethiopian Legal Basis	Responsible Authority
Releasing transaction-related information	Identity (8.2); Qualification (8.3); Terms of use (8.4); Online reputation info (8.6); Product info (8.7)	Pre-contract disclosures incl. identity, price, payment methods	Platform Operator; Consumer Protection Authority

Table 2-14 Mapping the Assurance Elements: In Transaction Phases

Activity	Relevant ISO 3211 Assurance Element(s)	Ethiopian Legal Basis	Responsible Authority
Placement / confirmation of electronic order	Transaction document (8.8)	Buyer's right to receive order confirmation on a durable medium	Platform Operator (issuance); Consumer Protection Authority (if dispute occurs)
Choice of payment method	Multiple payment methods (8.9)	Disclosure of acceptable payment methods and fees (Electronic transaction proclamation)	Platform Operator
Payment for purchased products	Multiple payment methods (8.9); Payment security rule (8.10)	Encouragement of secure payment systems; security audit requirements	Platform Operator, MinT, NBE, INSA
Delivery of purchased products	Delivery rule (8.11)	Obligation to specify reasonable delivery time; cancellation right if unmet	Platform Operator
Customs clearance	Customs clearance rule (8.12)	No explicit regulation for e-commerce customs integration	Ethiopian Customs Commission
Receipt with delivery confirmation	Delivery rule (8.11)	Rights linked to confirmed receipt (return/refund eligibility)	Platform Operator

Table 2-15 Mapping the Assurance elements : Post-transaction Phases

Activity	Relevant ISO 32111 Assurance Element(s)	Ethiopian Legal Basis	Responsible Authority
Performance evaluation	Online reputation information (8.6); Performance evaluation rule (8.13)	Requirement to manage authenticity of reviews, maintain dispute history	Platform Operator; Consumer Protection Authority
Resolving disputes	Transaction document (8.8); Dispute resolution rule (8.14)	Obligation to provide remedies, dispute channels, and referral to authorities	Platform Operator; Consumer Protection Authority
Return of products	Return & refund rules (8.15)	Obligation to publish and register return/ refund policies; right of withdrawal	Platform Operator
Refund of payment	Return & refund rules (8.15)	Obligation to disclose refund and settlement procedures before contract	Platform Operator
Compensation for transaction loss	Transaction document (8.8); Compensation rules (8.16)	Compensation for non-performance or defects	Platform Operator; Courts (in case of disputes)
Maintenance & technical support	Maintenance & technical support rule (8.17)	Obligation to provide maintenance/repair and penalties for non-compliance	Relevant Supervisory Authority (inspection & enforcement)

2.5.2. Mapping ISO 32111 Transaction Assurance Elements to Ethiopia's Legal and Institutional Framework

ISO 32111 establishes a structured approach to e-commerce transaction assurance based on three core components: principles, participants, and assurance elements covering all stages of a transaction. To evaluate how Ethiopia can operationalize transaction assurance in line with international best practices, the key assurance elements in ISO 32111 were mapped against existing Ethiopian legislation and draft directives, including the Electronic Transactions Proclamation No. 1205/2020, the Consumer Protection Directive for E-Commerce (Draft), the Commercial Registration and Licensing Proclamation No. 980/2016, and the Personal Data Protection Proclamation No. 1321/2024.

This comparison reveals that Ethiopia has already laid substantial legal foundations—

such as business registration, consumer disclosure obligations, data protection requirements, and dispute resolution mechanisms. However, these provisions are dispersed across multiple laws and are not yet structured into an integrated transaction assurance system. In particular, there is a lack of standardized implementation procedures, verifiable compliance mechanisms, performance indicators, and certification processes that could support a national trustmark system.

For example, under the ISO assurance element “Identity Information (8.2)”, Ethiopian law already requires e-commerce businesses to register their legal name, address, license status, and ownership structure through the commercial registration authority. However, this information is not publicly accessible in a consumer-friendly manner, nor is it integrated with online platforms or APIs. To meet ISO 32111 standards, it is recommended that the Ministry of Innovation and Technology (MinT), in coordination with the commercial registry, develop a publicly accessible business verification portal linked to platform registration data.

Similarly, “Qualification Information (8.3)” —which refers to verifying the legal and technical competence of e-commerce operators—is partially reflected in Ethiopia’s licensing system. Yet, there is no dedicated conformity assessment scheme for e-commerce platform security, digital service quality, or operational reliability. Therefore, it is recommended to develop a Platform Conformity Assessment and Certification Scheme, incorporating requirements such as secure payment processing, data protection compliance, software reliability, and consumer complaint handling.

Under “Terms of Use (8.4)”, Ethiopia’s Electronic Transactions Proclamation mandates disclosure of key contractual information before a transaction is finalized (Article 28). However, ISO standards call for standardized, transparent, and easily understandable formats —potentially in multiple languages—which are currently missing. This gap could be addressed by issuing model terms of service templates and plain-language summaries, led by MinT and the Consumer Protection Authority.

In the area of “Delivery Rules (8.11)”, Ethiopian regulations require platforms to state their delivery policies and maintain contracts with logistics providers. Yet, there are no formal Service Level Agreements (SLAs) for delivery times, delays, liability for loss or damage, or compensation procedures. To align with ISO 32111, MinT, Ethiopia Postal Service, and logistics regulators should establish standard delivery performance benchmarks, including minimum delivery timeframes, tracking requirements, and compensation rules.

Finally, while “Privacy and Data Protection” is covered under the 2024 Personal Data Protection Proclamation, there is no explicit linkage between data protection compliance and e-commerce platform certification. To ensure alignment with ISO standards, data protection compliance should be incorporated into annual platform audits, breach notification protocols, and personal data handling guidelines.

This mapping exercise shows that Ethiopia already meets the legal preconditions for transaction assurance but lacks an operational framework that converts laws into verifiable standards and certifiable trust mechanisms. ISO 32111 provides a foundation for this by defining:

- What must be assured (identity, payment security, delivery, dispute resolution, etc.)
- How assurance can be demonstrated (documentation, monitoring, audits, transparency)
- Who is responsible (platforms, regulators, certification bodies)

Table 2-16 Mapping ISO 32111 Transaction Assurance Elements to Ethiopia's Legal and Institutional Framework

ISO 32111 Assurance Element	Ethiopian Legal Source	Article/Clause	How It Relates	Responsible Authority
8.2 Identity Information	E-Commerce Consumer Protection Directive (draft)	Registration requirements— company name, address, license, TIN, representative details	Platforms must register and provide verifiable identity details before operation	MinT
	Commercial Registration & Licensing Proclamation No. 980/2016	Art. 5— No business license without commercial registration	Establishes legal identity of businesses	MoTRI
8.3 Qualification Information	Proclamation No. 980/2016	Art. 10— Certificate of competence	Businesses must prove competence before licensing	Sectoral authorities + MoTRI
	E-Commerce Directive	Renewal requires updated business license & tax compliance	Ensures continuous qualification compliance	MinT
8.4 Terms of Use/ Pre-contract Information	Electronic Transactions Proclamation (referenced in Directive)	Section 28— Pre-contract information requirements	Platforms must disclose terms, pricing, contract conditions before purchase	MinT
8.5 Third-party Service Rules	E-Commerce Directive	Requirement to provide security reports from recognized cybersecurity agencies	Applies to external payment, logistics, IT service providers	MinT, INSA or Accredited Cybersecurity Agency

ISO 32111 Assurance Element	Ethiopian Legal Source	Article/Clause	How It Relates	Responsible Authority
8.6 Online Reputation & Review Integrity	E-Commerce Directive	Platforms must monitor/remove fake or misleading reviews	Protects consumers from false reputation signals	MinT, Consumer Protection Authority
8.7 Product Information	E-Commerce Directive	Product description, price, delivery, payment conditions must be clearly shown	Ensures transparency of products offered online	Platform Operators, MinT
8.8 Transaction Documentation	E-Commerce Directive	Buyers have the right to receive order confirmation in durable form (email/SMS)	Ensures verifiable proof of transaction	Platforms
8.9 Multiple Payment Methods	E-Commerce Directive	Platforms must disclose acceptable payment methods and additional fees	Increases transparency and consumer choice	Platforms
8.10 Payment Security Rules	E-Commerce Directive	Cybersecurity assessment required during licensing and renewal	Ensures transaction-related security in payment systems	MinT, NBE
8.11 Delivery Assurance	E-Commerce Directive	Delivery terms must be disclosed; buyer has cancellation right if delivery fails	Protects consumer in logistics phase	Platforms, Logistics providers
8.12 Customs Clearance	Not yet regulated explicitly	–	No explicit legal provision found	Ethiopian Customs Commission
8.13 Performance Evaluation	E-Commerce Directive	Platforms must record disputes and make data available to regulators	Allows monitoring of platform reliability	MinT, Consumer Protection Authority
8.14 Dispute Resolution (ADR/ODR)	E-Commerce Directive	Platforms must provide dispute resolution channel & report to authorities	Supports fair resolution of conflicts	Platforms, Consumer Protection Authority

ISO 32111 Assurance Element	Ethiopian Legal Source	Article/Clause	How It Relates	Responsible Authority
8.15 Return & Refund Rules	E-Commerce Directive	Platforms must provide clear return/refund policies and allow withdrawal	Enables post-transaction consumer protection	Platforms
8.16 Compensation Rules	E-Commerce Directive	Consumer has right to compensation for non-conformity or failed delivery	Aligns with ISO's requirement for redress	Platforms, Civil Courts
8.17 Maintenance & Technical Support	Commercial Registration & Licensing Proclamation No. 980/2016	Duty to provide after-sales service/ maintenance where applicable	Supports long-term transaction assurance	Sectoral regulators, Platforms
(Cross-cutting) Privacy & Data Protection	Personal Data Protection Proclamation No. 1321/2024	Articles on lawful collection, processing, storage, breach notification	Protects personal data in all transaction phases	INSA, MinT
(Cross-cutting) Accessibility	E-Commerce Directive / Draft e-Transaction Regulation	Requirement to make terms & platform functions understandable	Supports ISO principle of accessibility	Platforms, MinT
(Cross-cutting) Accountability	Draft e-Transaction Regulation	Platforms must maintain records, cooperate with regulators, ensure compliance	Aligns with ISO accountability principle	MinT
(Cross-cutting) Authenticity	Draft e-Transaction Regulation	Prohibition of fake identity/product information	Aligns with ISO authenticity principle	Platforms, MinT

2.5.3. An Action Plan to Develop eTrust Mark Certification in Ethiopia

Developing an Ethiopian eTrust Mark should be grounded in clear governance arrangements, appropriate legal or policy authority, and alignment with international standards. Ethiopia can introduce the eTrust Mark Certification through two feasible voluntary pathways—Pathway A, a law-based model inspired by Korea, and Pathway B, a standards-based model centered on ISO alignment and market choice. Both pathways

can coexist, allowing Ethiopia to begin with a flexible approach while building toward a comprehensive transaction assurance ecosystem. Below, each pathway is presented through a four-step action plan.

Pathway A: a Law-Based Voluntary Certification Model inspired by ROK eTrust Mark

Unlike a mandatory licensing regime, Korea's eTrust certification system was voluntary but legally authorized, ensuring credibility and enforceability without imposing mandatory licensing. Ethiopia can adopt a similar model by embedding explicit certification authority in the Electronic Transactions Proclamation or a dedicated Ministerial Regulation.

① Step 1: Establish Legal Authority for Voluntary Certification

The first step is to formalize Ethiopia's legal mandate for voluntary e-commerce certification.

For instance, Drawing on Korea's Framework Act on Electronic Documents and Transactions (Articles 18, 18-2, 18-3, 22), Ethiopia may create provisions that:

- empower MinT to certify “excellent e-commerce business entities” (parallel to Article 18(1));
- authorize MinT to collect reasonable fees for certification (Article 18(2));
- define the use of certification marks and prohibit unauthorized use (Article 18-2);
- provide grounds for revocation of certification when operators fail to meet required criteria (Article 18-3);
- designate or establish a national secretariat responsible for supporting certification work (Article 22: Korean designated agency).

This creates a clear legal mandate while keeping participation voluntary for platforms.

Then, a national technical committee—led by the Ministry of Innovation and Technology (MinT) and including ECA, the Consumer Protection Authority, the National Bank of Ethiopia, logistics regulators, and customs authorities—should be established to localize the structure of ISO 32111 (transaction assurance principles, participants, and assurance elements) and ISO 32112 (evaluation indicators) into Ethiopia's regulatory ecosystem. This localization process will convert ISO assurance principles into enforceable Ethiopian rules, defining minimum thresholds for identity verification, data protection (aligned with Proclamation No.1321/2024), disclosure, delivery assurance, dispute resolution, and performance evaluation, as discussed in the Sub-Sections 2.5.1 and 2.5.2.

② Step 2: Assign Institutional Roles and Build National Audit Capacity

Following the Korean model—where a designated agency supported the Minister through certification operations—Ethiopia may establish a national coordinating body,

tentatively called “a National eCommerce Transaction Assurance Secretariat” under MinT, which will be responsible for administering the eTrust Mark system. Key responsibilities include:

- Accrediting and training auditors in ISO-based assessment methods (processing capacity, interface quality, data integrity, security controls, refund timelines, delivery traceability)
- Managing certification applications, audits, dispute mediation, and monitoring
- Maintaining a public registry of certified businesses
- Coordinating with the Consumer Protection Authority, NBE (for payment security), and logistics agencies
- Allowing future accreditation of independent certification bodies, in line with international conformity assessment practice

In particular, capacity building must include auditor training on ISO-based indicators—processing capacity, interface quality, data integrity, security measures (ISO/IEC 27001 reference), refund timeliness, logistics traceability, and sustainability. This ensures that Ethiopia develops a sustainable pool of technical assessors and a strong institutional foundation.

In addition, following the Korean model—where NIPA acted as the certification operator and the Dispute Mediation Committee supported enforcement—Ethiopia may create a Dispute Mediation Committee as part of the legal framework.

③ Step 3: Create a Structured, Law-Based Certification Procedure

Based on Korea's Enforcement Decree Article 2-2, Ethiopia can establish:

- certification criteria (usability, safety, privacy protection, transaction process integrity, delivery/return policies, information transparency, system security, and compliance with consumer protection laws);
- required documentation (including terms of use, business registration, consumer protection arrangements, and system security proof);
- application and screening procedures;
- issuance of certification and validity period (e.g., one-year cycle);
- monitoring obligations and revocation criteria;
- requirements for displaying the eTrust Mark, mirroring Article 18-2(1) of Korea's Act.

In addition, Ethiopia can establish a structured process that enhances transparency and predictability:

Table 2-17 eTrust Mark: Suggested Procedure for Pathway A

1. Application Submission

Platforms provide documents similar to those required under Korea's Enforcement Decree Article 2-2(2): compliance evidence, business plan, and terms of use.

2. Self-Assessment and Disclosure

Platforms conduct a self-check against ISO 32112 indicators and Ethiopia's adapted assurance rules.

3. Formal Audit and Scoring

Audits evaluate compliance with assurance elements including:

- identity verification
- payment security
- delivery and customs assurance
- refund/return procedures
- personal data protection
- system resilience and security logs
- review authenticity

Following Korea's Article 18(3), audits should verify adherence to certification standards defined by regulation.

4. Certification Decision and Issuance

A one-year certification period is recommended, mirroring Korea's eTrust model.

5. Monitoring and Possible Revocation

Ethiopia should incorporate revocation rules similar to Article 18-3, allowing cancellation for example when:

- certification was obtained fraudulently
- operators violate required behaviors
- they fail to maintain certification standards

④ Step 4: Introduce Nationwide Consumer and Business Awareness Efforts

To ensure impact, the certification must be clearly recognized and trusted by consumers. Ethiopia should implement:

- National campaigns explaining the meaning, benefits, and verification methods of the eTrust Mark.
- Public promotion of certified platforms.
- SME-focused guidance on meeting certification requirements.
- A standardized dispute resolution channel and public registry of certified platforms.

Korea's experience shows that widespread recognition of the trustmark significantly strengthened consumer confidence. Ethiopia can achieve similar outcomes through coordinated awareness efforts led by MinT.

Awareness initiatives may reference Korea's approach of requiring certified platforms to display a standard information page and maintaining a public registry of certified entities. Over time, increased visibility will strengthen consumer trust and incentivize platforms to pursue certification voluntarily.

Pathway B: An International Standard-Aligned, Voluntary Trustmark System

Pathway B offers an ISO-based, standards-driven, fully voluntary trustmark system, requiring no immediate legal amendments. This approach allows Ethiopia to move rapidly by relying on national standards, accredited conformity assessment bodies (CABs), and market incentives. It mirrors global best practices where trustmarks operate as industry-led certification schemes aligned with ISO and overseen by the national standards body. This pathway emphasizes consistency with global standards while maximizing flexibility for businesses. This pathway utilizes ISO 32111 and ISO 32112, with the Ethiopian Standards Agency (ESA) leading the development of a national Ethiopian Standard and accrediting conformity assessment bodies. The eTrust Mark is issued voluntarily to platforms that meet the national standard.

Under this pathway, the Ethiopia Standards Agency (ESA)—as the national standards body—would:

- Develop an Ethiopian Transaction Assurance Standard aligned with ISO 32111/32112
- Host technical committees with representations including MinT, the Ethiopian Communications Authority (ECA), the Consumer Protection Authority, the National Bank of Ethiopia (for payment security oversight), Ethiopian Customs Commission (cross-border delivery and customs assurance), Ethiopian Postal and Logistics operators, Private-sector e-commerce platforms, fintechs, and Civil society groups specializing in digital rights and consumer protection
- Issue conformity assessment guidelines
- Accredite certification bodies

- Maintain national standard documentation and facilitate future revisions

This avoids overburdening legislation while enabling international harmonization.

① Step 1: Develop Ethiopian National Standards Based on ISO Frameworks

ESA should create an official Ethiopian Standard (i.e. ES xxxx: Transaction Assurance for E-Commerce) using ISO 32111 (principles and assurance elements) and ISO 32112 (evaluation indicators) as the normative basis.

A Technical Committee on E-Commerce Assurance should be established under ESA, with members from:

- Ministry of Innovation and Technology (MinT)
- Ethiopian Communications Authority (ECA)
- Consumer Protection Authority
- National Bank of Ethiopia (for payment assurance and security)
- Ethiopian Customs Commission (delivery and customs assurance)
- Ethiopian Postal and Logistics operators
- Private-sector e-commerce platforms, fintechs, and logistics firms
- Civil society groups specializing in digital rights and consumer protection

This committee would:

- Translate ISO 32111's assurance principles into Ethiopia-specific clauses
 - Identity verification requirements for sellers and platforms
 - Transparency of fees, delivery timelines, and return policies
 - Authenticity and integrity of information (product specs, reviews)
 - Security and privacy requirements aligned with Ethiopia's PDP Proclamation No.1321/2024
- Adopt measurable indicators from ISO 32112 to ensure that certification is evidence-based, including:
 - Platform performance
 - Transaction efficiency
 - Security controls and incident-handling procedures
 - Refund timelines
 - User satisfaction metrics
 - Delivery success rates
- Define conformity assessment methods in national standards, including:
 - Documentation review requirements
 - On-site/remote technical audit procedures
 - Sampling methods for testing transaction processes
 - Scoring mechanisms and pass thresholds

- Tailor global standards to Ethiopia's market context including:
 - Integration with mobile money systems
 - Consideration of informal logistics networks
 - Limited digital literacy among SMEs
 - Local languages and accessibility needs

This step produces a recognized national standard enabling transparent and consistent certification.

② Step 2: Build Certification Capacity Without Legal Mandate

Because Pathway B is voluntary, Ethiopia should ensure credible certification operations even without formal legal authority.

ESA plays a central role as Ethiopia's national standards body, responsible for:

- Accrediting Conformity Assessment Bodies (CABs),
- Training auditors
- Coordinating with Mint/ECA
- Engaging industry bodies for early implementation

CABs may include: 1) MinT acting as a certification body; 2) ECA (technical compliance audits); 3) Private accredited auditors; and 4) Industry associations. Accreditation follows ISO/IEC 17065 (Certification of Products, Processes, and Services).

To training auditors, ESA develops training curricula covering:

- ISO 32111/32112 requirements
- Assurance element verification methods
- Digital platform auditing techniques
- Payment and cybersecurity controls
- Complaint-handling and dispute assessment

Although Pathway B is not law-based, MinT and ECA offer:

- Market guidance
- Policy alignment
- Coordination with digital transformation programs

Like Korea's early-stage approach—where e-commerce associations operated parts of the trustmark scheme—Ethiopia can engage Industry Bodies for Early Implementation. For instance, industry bodies such as Ecommerce associations, ICT federations, Digital innovation hubs can be designated as initial certification facilitators. This ensures the certification ecosystem grows rapidly without requiring new law.

③ Step 3: Implement a Voluntary Certification Process

Pathway B's certification follows an internationally recognizable five-step process, suitable for both large platforms and SMEs.

Table 2-18 eTrust Mark: Suggested Procedure for Pathway B

1. Application Submission

Platforms submit documentation including:

- Business registration
- Terms of use
- Privacy and security policies
- Evidence of internal controls
- Contact and ownership information
- Delivery/return/refund policies
- System architecture overview

ESA publishes a national application template to standardize submissions.

2. Self-Assessment Using Ethiopian Standard Checklists

Platforms score themselves using:

- ISO 32112-derived indicators
- Ethiopian Standard assurance requirements
- Supporting evidence (screenshots, logs, process documents)

Self-assessment promotes:

- Early gap identification
- Reduced audit costs for SMEs
- Transparent expectations before formal assessment

3. Formal Audit and Scoring by Accredited CABs

Audits include:

1) Document Review

- Terms of use
- Payment integration
- Customer support systems
- Internal processes
- Refund workflows

2) Technical Assessment

- Website/mobile app usability
- System security and authentication
- Logging and incident-handling procedures
- Transaction flow tests

3) Operational Assessment

- Delivery tracking
- Complaint-handling mechanisms
- Return logistics

4) Audit scoring uses ISO 32112 metrics such as:

- Availability
- Refund cycle time
- User satisfaction metrics
- Processing time per transaction
- Fraud detection capability

4. Certification Decision and Issuance

CAB issues:

- A one-year eTrust Mark certificate
- A digital badge for platform display
- A summary compliance report for consumers

ESA maintains an official National Registry of Trusted E-Commerce Platforms.

5. Monitoring and Renewal

Monitoring procedures include:

- Periodic reporting
- Incident reporting requirements
- Mystery-shopping style audits
- Annual audit for renewal

Serious non-compliance leads to:

- Suspension
- Revocation of certificate
- Public notice

Since certification is voluntary, the main enforcement tool is market reputation, not legal penalties.

This creates a rules-based trustmark system grounded in international assurance principles and supported by international precedents.

④ Step 4: Market Education Through Incentives, Not Regulation

In Pathway B, adoption grows through market incentives, not mandatory rules.

Government-led incentives may include the following:

- MinT publishes a Trusted Platforms List on official portals.
- Preferential search ranking or promotional placement in national digital marketplaces.
- Reduced audit fees for SMEs or startups.
- Optional integration with government procurement platforms (e.g., Buy-From-Ethiopia programs).

Consumer-facing campaigns may include the following:

- Public awareness initiatives explaining the meaning and benefits of the eTrust Mark.
- Collaboration with national telecom operators for SMS or app-based awareness campaigns.
- Social media campaigns featuring certified platforms as best-practice examples.

Industry incentives may include the following:

- Platforms use certification for marketing and competitive advantage.
- Logistics and payment service providers partner preferentially with certified platforms.

For cross-border value, the Alignment with ISO 32111/32112 may enable potentially easier international recognition under AfCFTA Digital Trade Protocol.

Pathway B thus produces a flexible, business-friendly, internationally aligned trustmark ecosystem suitable for rapid deployment.

2.5.4. Suggested Timeline for Rollout

A phased rollout allows Ethiopia to develop the institutional, legal, and technical foundations necessary for a national trustmark regime.

Year 1 — Legal Authorization, Standard Development, and Pilot Audits

- Draft and insert legal clauses enabling voluntary government certification (referencing Korea's Articles 18–18-3 and Article 22).
- ESA initiates development of the Ethiopian Standard for E-Commerce Transaction Assurance aligned with ISO 32111/32112.
- Train the initial cohort of auditors under MinT/ECA oversight.
- Conduct pilot audits with 3–5 platforms to validate certification indicators and procedures.
- Publish guidance for SMEs regarding requirements and benefits.

Year 2 — Formal Launch of the Voluntary eTrust Mark Certification

- Officially launch the certification scheme, publish criteria, and open applications.
- Establish the National eCommerce Transaction Assurance Secretariat to manage applications and audits.
- Begin issuing annual certifications, enabling certified businesses to display the mark.
- Expand stakeholder training: logistics providers, payment service providers, SMEs.

- Build a public verification page listing certified businesses.

Year 3 — Expansion, Enforcement of Mark Usage, and Regional Alignment

- Introduce penalties for misuse of the eTrust mark (referencing Korea's Article 18-2(2)).
- Integrate the trustmark into public procurement or government digital platforms (voluntary but incentivized).
- Launch cross-border cooperation discussions under AfCFTA Digital Trade Protocol for recognition of trust mechanisms.
- Evaluate system performance using ISO 32112 indicator frameworks.

Year 4 and Beyond — Institutionalization and International Cooperation

- Expand auditor pools, possibly accrediting independent certification bodies.
- Consider introducing a light-tier certification for SMEs to reduce compliance burdens.
- Pursue mutual recognition with African trustmark bodies to facilitate cross-border e-commerce.
- Annual revision of guidelines based on market feedback and dispute mediation cases.

2.5.5. Addressing Implementation Challenges

Cost Burdens for SMEs

- Introduce tiered certification levels (Basic/Standard/Premium)
- Provide subsidized training or audits for micro and small enterprises

Regulatory Capacity Constraints

- Use ESA as the national standards body to lead the technical development of certification requirements
- Utilize MinT/ECA as the administrative authority, referencing Korea's dual structure (ministry + designated agency)

Consumer Awareness Gap

- Deploy long-term digital literacy campaigns
- Partner with telecom operators and digital marketplaces to promote certified platforms

Legal Framework for E-Commerce: Draft Directives and Commentary

3.1. Introduction: Rationale for Priority Legal Instruments

Ethiopia's e-commerce economy is expanding rapidly, but the legal framework remains fragmented and payment centric, leaving core parts of the online transaction cycle either under regulated or not regulated at all. While important building blocks such as the Electronic Transactions Proclamation, the National Payment System Proclamation, and the new Personal Data Protection Proclamation are in place, there is still no dedicated, end-to-end e-commerce law that clearly regulates platform-based trade, consumer rights, logistics, and intermediary responsibilities in a coherent manner.

Current framework and practical gaps

Today, platforms such as Zemen Gebeya (B2C marketplace), Jiji (C2C classifieds), ChipChip (social group buying) and AfrotieGari (vehicle classifieds) all operate under generic electronic transactions rules, even though their risk profiles and roles in the value chain are very different. When a consumer buys a defective car via Jiji or spoiled vegetables via ChipChip, the law does not clearly indicate whether the platform is merely a messaging board or whether it owes specific duties of seller verification, transparency, and complaint handling, which leads to uncertainty and inconsistent outcomes.

Intermediary liability is another critical gap: there is no explicit safe harbour regime that ties limited liability to due diligence obligations such as seller KYC, notice and takedown, cooperation with authorities, or repeat infringer policies. As a result, informal trade via Telegram channels and Facebook Marketplace has flourished completely outside of licensing, tax and consumer protection oversight; for example, Telegram channels advertising “iPhones at factory price” can collect advance payments via Telebirr and disappear, with no clear allocation of legal responsibility between the channel operator, the platform and payment providers.

Consumer protection, logistics and data protection practice also show significant weaknesses. Many online sellers provide minimal contact details, vague or non-existent return and refund policies, no structured complaints process, and no neutral online dispute resolution, forcing consumers to rely on personal negotiation or “naming and shaming” on social media when problems arise. At the same time, customs rules are not yet adapted to small B2C parcels, which constrains the full use of the new Ethiopian Airlines e-commerce hub at Bole, and there is no e-commerce specific regime for cybersecurity standards, breach notification, or incident response for platforms handling large volumes of user data.

Alignment with AfCFTA and need for a structured framework

Ethiopia has already taken important steps that align with the AfCFTA Digital Trade Protocol, notably on digital ID, electronic transactions, data protection, and digital payments, which correspond broadly to Articles 14–21 of the Protocol. However, domestic rules remain underdeveloped in key AfCFTA areas such as logistics and last mile delivery (Article 11), electronic invoicing and e-receipts (Article 13), online consumer protection (Article 27), MSME inclusion and digital participation, and innovation sandboxes for fintech and e-commerce (Articles 30–35). This gap explains why a more comprehensive e-commerce legal architecture is needed, built around a sequence of targeted directives and, in the medium term, a framework e-commerce law.

Why these two directives are prioritized

Against this background, the Ministry of Innovation and Technology has requested two foundational directives as first-generation instruments: (i) an E-Commerce Licensing and Registration Directive, and (ii) an Intermediary Liability Directive.

The E-Commerce Licensing and Registration Directive is designed to answer a basic but currently unresolved question in the Ethiopian system: “who must be inside the regulatory perimeter, under what license, and subject to which minimum entry and conduct standards?” It establishes clear categories such as electronic platform operators and intra-platform operators, sets eligibility requirements linked to incorporation, tax registration, business integrity and technical capability, and creates predictable procedures for application, review, renewal, and suspension or revocation. In practical terms, this means that large marketplaces, dedicated e-retailers and fulfilment platforms will be subject to a robust licensing regime, whereas small social commerce sellers and occasional C2C traders can be handled through lighter touch registration, thus balancing MSME inclusion with traceability and consumer protection.

The Intermediary Liability Directive, in turn, provides the missing legal backbone on when and how intermediaries such as ISPs, hosting services, search engines, marketplaces, payment platforms and participative platforms can be held liable for

third party content and transactions. It defines categories of intermediaries, introduces conditional safe harbour rules linked to concrete due diligence obligations (for example, verifiable seller onboarding and KYC, effective notice and takedown and repeat infringer policies, and structured cooperation with law enforcement authorities), and clarifies the treatment of “neutral” versus “active” platforms that exert control over pricing, presentation, fulfilment or payment flows. This directly addresses recurring problems such as counterfeit pharmaceuticals sold on marketplaces, fraudulent investment schemes promoted through online platforms, or dangerous products reaching minors, all of which currently fall into grey zones of responsibility.

Role of the two directives in the broader roadmap

These two directives are deliberately framed as foundational building blocks of a broader e commerce legal framework rather than as isolated instruments. By clarifying who needs a license, how they enter and remain in the system, and what baseline responsibilities intermediaries owe to consumers and public authorities, they create the necessary legal and institutional “rails” on which more specialized instruments—such as detailed online consumer protection rules, logistics and fulfilment standards, cross border e commerce procedures, and certified online dispute resolution schemes—can be added in subsequent phases.

In addition, the two directives are drafted to be fully compatible with Ethiopia's existing electronic transactions, payment system and data protection laws, and to support gradual implementation of AfCFTA Digital Trade Protocol commitments on online consumer protection, data governance, cybersecurity and MSME participation, without stifling innovation in a still fragile e commerce ecosystem.

In this First-Year Consultation Report, the draft texts of the two priority legal directives are presented to illustrate the core legal outputs of the consultation. Detailed article-by-article explanations, institutional analysis, and practical implementation considerations are provided separately in the document titled “[Year 1 Deliverables] Draft E-Commerce Directives and Commentary,” which has been prepared as a standalone legal deliverable for practical reference and policy discussion. This separation is intended to enhance the usability of both documents, allowing the present report to focus on overall context and structure, while the companion deliverable supports in-depth legal review.

3.2. Intermediary Liability Directive (Draft)

PART I. GENERAL PROVISIONS

Article 1. Short Title

This Directive may be cited as the “Intermediary Liability Directive”.

Article 2. Purpose

To establish the legal framework governing the liability of Internet Intermediaries, fostering innovation, economic development, consumer protection, and compliance with public policy.

Article 3. Scope

Applies to all intermediaries operating in Ethiopia and covers activities relating to hosting, transmitting, indexing, networking, search, e-commerce, web platforms, and payment systems.

Article 4. Definitions

‘Intermediary’, ‘Hosting provider’, ‘Conduit provider’, ‘Notice and Take-Down’, ‘User-generated content’, ‘Illegal content’, ‘Personal Data’, ‘Consumer’, and other relevant terms.

Article 4 – Definitions (excerpt for key terms)(Revised)

1. Illegal content means any information, data, or communication that violates a specific, clearly published provision of Ethiopian law, including the Criminal Code, the Computer Crime Proclamation, the Media Proclamation, the Personal Data Protection Proclamation, or any other statute or regulation duly published in the Federal Negarit Gazette.
Content shall not be considered illegal solely because it is controversial, critical of public authorities, or politically sensitive, unless it clearly falls within the scope of an offense defined by Ethiopian law.
2. Actual knowledge means that an intermediary has received either
 - a. a valid order issued by a court or other competent authority identifying specific content as illegal and requiring action; or
 - b. a formal notice that meets the minimum statutory requirements, including identification of the notifier, precise technical locator (such as URL) of the content, the specific legal provision allegedly violated, and a brief factual explanation of the alleged illegality.

Mere informal complaints, general allegations, or vague user reports that do not satisfy these requirements do not, by themselves, constitute actual knowledge.

3. Significant platform means an intermediary that meets one or more thresholds established by regulation, including but not limited to:
 - a. a minimum average monthly number of active users in Ethiopia;
 - b. an annual turnover derived from activities in Ethiopia above a specified amount;or
 - c. a formal designation by the Ethiopian Communications Authority based on the platform's systemic impact on users, markets, or public interests.
4. User generated content, indexing, search services, and participative platforms shall be defined in a technology neutral manner, focusing on their functional role in enabling users to create, access, organize, or share content, regardless of the specific technical architecture or interface.

Article 5. Application

Intermediaries covered under this directive include ISPs, hosting services, search engines, e-commerce, payment, and participative platforms.

Article 6. Exemptions

Excludes intermediaries solely providing telecommunications infrastructure, or state-mandated emergency communication services.

Article 7. Interpretation

Interpretations shall favor transparency, proportionality, and protection of innovation and users' rights.

Article 8. Relationship with Other Laws

This directive complements the Electronic Transactions Proclamation, Consumer Protection Proclamation, existing criminal statutes, and data protection regulations.

PART II. LIABILITY PRINCIPLES

Article 9. Limited Liability Principle

Intermediaries are not liable for third-party content unless they have initiated it or failed to act upon actual knowledge of illegal activity.

Article 9 — Limited Liability Principle (revised)

1. Intermediaries shall not be liable for third party or user generated content that they

- transmit, cache, or host, provided that they act neutrally and do not initiate, select, or modify the content, and provided that they comply with this Directive once they obtain actual knowledge of illegal content as defined in Article 4.
2. Liability shall arise where an intermediary
 - a. initiates, edits, or otherwise makes third party content its own; or
 - b. obtains actual knowledge of specific illegal content and fails to act within the time limits and procedures established under this Directive.
 3. For the purposes of this Article, an intermediary that receives vague, incomplete, or anonymous complaints shall be entitled to request additional information and shall not lose safe harbour protection solely because it has been informed in general terms that some content “may be unlawful”.

Article 10. Conduit Exemption

Conduit providers that do not initiate, select, or modify transmitted data are exempt from liability.

Article 11. Caching Exemption

Providers caching information are not liable if operating automatically, not modifying information, and updating as necessary.

Article 12. Hosting Exemption and Obligations

Hosting providers are not liable for stored user content except where they have actual knowledge of unlawful material and fail to act expeditiously.

Article 12 — Notice and Takedown (revised structure)

1. Valid notice

A notice of allegedly illegal content shall be considered valid if it contains at least:

 - a. the full name and contact details of the notifier or its authorized representative;
 - b. a precise URL or other unique locator of the content in question;
 - c. the specific Ethiopian legal provision allegedly violated; and
 - d. a brief factual explanation of why the content is considered illegal under that provision.
2. Deadline for action

Unless a shorter period is specified in a court or authority order, intermediaries shall act on valid notices and relevant orders within forty eight (48) hours of receipt, either by removing or disabling access to the content, or by providing a reasoned response explaining why no action is taken.
3. Record keeping and transparency

Intermediaries shall keep records of notices, actions taken, and any counter notices

or appeals for a minimum period defined by regulation, while complying with applicable data protection law.

4. Abusive notices

Where an intermediary or competent authority identifies clearly false, fraudulent, or bad faith notices, proportionate sanctions may be imposed on the notifier, including administrative fines or loss of trusted notifier status, without prejudice to civil or criminal remedies.

5. User appeal and counter notice

Users whose content has been removed or restricted shall have access to a simple and timely counter notice and appeal mechanism, the basic parameters of which shall be further elaborated by regulation.

Article 13. Search and Link Exemption

Search engines and link aggregators are exempt if engagement is passive, not editorial, subject to exceptions defined for unlawful activity.

Article 14. No General Monitoring Requirement

No intermediary shall be subject to a general obligation to monitor or actively seek illegal activity beyond specific legal requirements.

Article 15. Safe Harbour Criteria

Principles for safe harbour include transparency, notice process, counter-notice, and fair dispute resolution.

Article 16. Notice and Takedown System

Standardizes procedures for notice and takedown: form, content, evidence, timelines, counter-notice, and record keeping.

Article 17. Repeat Infringer Policy

Providers must implement policies for handling repeat infringement, including possible suspension, notice, and appeals for affected users.

PART III. SPECIAL LIABILITY CASES

Article 18. Intellectual Property Protection

Intermediaries must expeditiously remove copyrighted or trademark-infringing material upon verified notice from rights holders.

Article 19. Child Protection Obligations

Immediate removal, blocking, or reporting of child sexual abuse material is mandated.

Article 20. Consumer Protection Compliance

Obligations to facilitate transparent advertising, dispute resolution, returns, and refunds, as required by consumer protection law.

Article 21. Counterfeit Goods Prevention

Intermediaries must act on authority notice concerning counterfeit goods and cooperate with relevant enforcement agencies.

Article 22. Cybersecurity and Malware

Obligation to act on authority or user reports for removal and communication regarding malware, phishing, or security threats.

Article 23. Unlawful Gambling and Prohibited Services

Intermediaries must block access to illegal gambling or any service proscribed by Ethiopian law, upon notification.

Article 24. Hate Speech and Defamation

Providers must expeditiously remove content found to constitute hate speech or defamation by competent authority or court order.

Article 24 — Hate Speech (clarified cross reference)

1. For the purposes of this Directive, hate speech shall be understood in line with the offenses defined under the Ethiopian Criminal Code and Media Proclamation, including elements such as intent, identification of protected groups, and likelihood of causing serious harm.
2. Platforms shall not be required to remove content merely because it is critical of public authorities, expresses minority views, or is politically contentious, unless it clearly meets the statutory criteria for hate speech offenses.

Article 25. National Security Content

Compliance with lawful orders for immediate removal or restriction of content impacting national security interests.

Article 25 — National Security (with safeguards)

1. Any order to remove, restrict, or block access to content or services on grounds of national security shall be

- a. made in writing;
 - b. specific as to the content, account, or service concerned; and
 - c. issued or authorized by a clearly designated high level authority identified by law.
2. Affected intermediaries and, where appropriate, users shall have the right to seek ex post judicial review of national security orders to assess their legality and proportionality.
3. Subject to necessary confidentiality, the competent authority shall publish periodic, aggregated transparency information on the number and type of national security related orders issued under this Article.

PART IV. USER PROTECTION AND PRIVACY

Article 26. Personal Data Handling

Requirements for data privacy, explicit consent, processing limitations, and secure storage in line with Ethiopian data protection laws.

Article 27. User Notification

Providers must notify users of content or account removal, reasons, appeals, and process for restoration or counter-notice.

Article 28. Appeal and Redress

Clear mechanisms for appeals against removals, suspensions, or other administrative actions by intermediaries.

Article 29. Confidentiality and Records

Procedures for maintaining confidentiality of user data, content removal records, and handling of law enforcement requests.

Article 30. Transparency Reports

Regular publication of reports on removal actions, requests received, and outcomes by significant platforms.

PART V. OPERATIONAL OBLIGATIONS AND ENFORCEMENT

Article 31. Duty of Care

Proportionate duties of care for specific content categories, subject to ministerial rules for child safety, security, and consumer rights.

Article 31 — Duty of Care (narrowed)(Revised)

1. Nothing in this Directive shall be interpreted as imposing a general obligation on intermediaries to monitor information which they transmit or store, or actively to seek facts or circumstances indicating illegal activity.
2. Any specific duties of care imposed on intermediaries shall
 - a. be explicitly defined in this Directive or in regulations adopted under it;
 - b. be narrowly targeted at clearly identified risks, such as known child sexual abuse material, high risk financial fraud schemes, or clearly identified malware; and
 - c. be proportionate to the size, technical capacity, and risk profile of the intermediary concerned.

Article 32. Cooperation with Authorities

Obligation to cooperate in lawful investigations; preservation and disclosure of records on request pursuant to law.

Article 33. Technical Standards

Providers shall comply with applicable standards for identifying, classifying, and filtering, where mandated.

Article 34. Complaint Resolution Mechanism

Mandates intermediaries to establish accessible mechanisms for resolving user and third-party complaints relating to content, service, or transactions.

Article 35. Staff and Contact Point

Designate staff and publish contact details for handling content and legal requests.

Article 36. Education and Awareness

Providers must support education and awareness programs on user rights, cybersecurity, safe internet use, and notice procedures.

Article 37. Implementation Guidance

Ministry may issue further guidance or regulations for technical implementation of notice, appeals, and compliance processes.

Article 38. Audits and Inspections

Intermediaries subject to periodic audits or inspections by authorities to verify compliance.

Article 39. Multi-stakeholder Review Board

Establishes a board to review directive effectiveness, address policy challenges, and advise on proposed amendments.

Article 40. Penalties for Non-compliance

Specifies penalties, fines, and remedial actions for breaches, proportional to the nature and impact of violations.

Article 41. Transitional Arrangements

Sets timelines and support mechanisms for existing providers to conform to new obligations.

Article 42: Entry into Force

This Directive shall take effect on the date of its publication in the Federal Negarit Gazette.

3.3. E-Commerce Licensing and Registration Directive (Draft)

PART I. GENERAL PROVISIONS

Article 1. Short Title

This Directive may be cited as the “E-Commerce Licensing and Registration Directive No. [____]/2025.” Its title and number shall be referenced in all legal documents and official communications.

Article 2. Purpose

This Directive establishes clear, fair, and transparent rules for licensing, operation, and supervision of e-commerce activities in Ethiopia, promoting innovation and ensuring consumer protection.

Article 3. Definitions

All key terms, including “e-commerce,” “platform operator,” “intra-platform operator,” “Ministry,” “licensee,” and “consumer,” are defined in the attached Schedule.

Article 3 — Definitions (excerpt)(Revised)

1. E-commerce means the commercial supply of goods or services to Ethiopian consumers through electronic means, including websites, mobile applications, social-media commerce, or other digital interfaces, regardless of the device or network used.
 2. Electronic platform operator means any person or entity that operates a digital interface which enables multiple, independent sellers or service providers to offer goods or services to consumers, whether or not the operator processes payments or temporarily holds goods.
 3. Intra-platform operator means a business or individual that offers goods or services through an electronic platform operated by a third party and does not own or control the platform itself.
- ※ These and related definitions shall be further elaborated in the Schedule, in a manner consistent with Ethiopian tax, consumer-protection, and data-protection legislation.

Article 4. Scope of Application

This Directive applies to all persons or entities—domestic and foreign—engaged in e-commerce activities aimed at Ethiopian consumers or conducted within Ethiopia's borders.

PART II. LICENSING AND REGISTRATION

Article 5. Licensing Categories

For the purposes of this Directive, the Ministry shall issue the following categories of licenses to regulate e-commerce activities:

- a) Electronic Platform Operator License (Code 85125),
- b) Intra-Platform Operator License (Code 85126),
- c) Other categories designated by the Ministry in response to market developments.

Article 6. Eligibility Requirements

Applicants must submit incorporation documents, TIN, proof of business integrity and technical capability, and ensure compliance with laws on consumer and data protection.

Article 6 — Eligibility Requirements (revised emphasis)

Applicants shall demonstrate:

- a. valid incorporation and tax registration; and
 - b. business integrity and technical capability, assessed on the basis of objective and verifiable criteria, including:
 - i. absence, within a defined look-back period, of final convictions for fraud, money-laundering, or tax evasion against key officers and beneficial owners;
 - ii. absence of unresolved sanctions imposed by major Ethiopian regulators; and
 - iii. minimum information-security and operational standards set by the Ministry.
- ✂ Detailed guidance on required documentation, such as tax clearance certificates and beneficial-ownership declarations, shall be published by the Ministry to ensure transparency and predictability.

Article 7. Application Submission

Applications must be submitted online or in person, with all supporting documents as required by the Ministry.

Article 8. Licensing Review and Determination

The Ministry shall notify applicants of approval or refusal within 30 working days. Additional information may be requested during review.

Article 9. Validity and Renewal

Licenses are valid for one year, renewable on ongoing compliance. Renewals must be submitted at least 30 days prior to expiry.

Article 10. License Suspension and Revocation

The Ministry may suspend or revoke licenses for non-compliance, fraud, misrepresentation, or significant risk to the public, with written notice and appeal opportunity.

Article 11. Provisional Licensing

Innovative, pilot, or experimental e-commerce models may operate under provisional licensing subject to stricter conditions and regular Ministry review.

Article 12. Licensing for Foreign Platforms

Foreign entities must appoint a local representative, register with the Ministry, and ensure VAT and other requirements are fulfilled for Ethiopian user protection.

PART III. MARKET OPERATIONS AND OBLIGATIONS

Article 13. Business Disclosure

Operators must display licensing and contact details, business registration, and terms of service on all digital interfaces in languages accessible to Ethiopian consumers.

Article 14. Governing Officers and Ownership

Operators must disclose and regularly update information regarding beneficial owners, directors, and responsible officers to ensure transparency.

Article 15. Security and Technical Standards

Platforms must meet minimum technical, security, and data protection standards as issued by the Ministry, and maintain up-to-date cybersecurity protocols.

Article 16. Integrity of Transactions

Operators must ensure that all transactions are accurately recorded, digitally tracked, and provided with electronic receipts.

Article 17. Advertising and Marketing

All marketing materials and offers must be clear, truthful, and not misleading; influencer and sponsored content must be labeled as such.

Article 18. Prohibited Activities

Unfair trade practices, sale of prohibited items, and facilitation of illegal activities through platforms are strictly forbidden.

✖ The list of prohibited activities under this Directive shall operate without prejudice to the Ethiopian Criminal Code and other applicable criminal statutes. Serious violations of this Directive may be referred to law-enforcement authorities for investigation and prosecution, while regulatory sanctions applied under this Directive shall remain distinct from criminal penalties and shall respect principles of proportionality and non-duplication.

Article 19. Third-Party Service Providers

Operators integrating logistics, payments, or ancillary services must ensure those providers are licensed and comply with sectoral regulations.

Article 19 — Third-Party Integration (due-diligence based)(Revised)

1. Platform operators shall exercise reasonable due diligence when integrating third-party logistics, payment, or other service providers, including verifying required licenses, keeping relevant records, and responding to substantiated complaints.
2. They shall not be strictly liable for all misconduct of independent partners; however, where a platform knows or clearly should know of persistent serious non-compliance by a partner and fails to take corrective measures, it may be subject to regulatory sanctions.

Article 20. AML/CFT Compliance

Platforms must implement customer due diligence, report suspicious activity, and cooperate with authorities to prevent money laundering and terrorist financing.

PART IV. CONSUMER AND DATA PROTECTION

Article 21. Consumer Right to Information

Consumers must be informed of total price, key contract terms, delivery timeframes, and return/refund policy before checkout.

Article 22. Order Fulfillment and Redress

Operators are responsible for order delivery as promised; complaints and refund requests must be acknowledged within 7 days and resolved promptly.

Article 23. Complaint Handling

A clear, accessible process must be provided for lodging complaints; unresolved issues may be escalated to statutory consumer authorities.

Article 24. Refunds and Returns

Refund and return processes must comply with published standards, with timelines clearly stated and enforced without unreasonable conditions.

Article 25. User Notification

Any limitation, removal, or suspension of user accounts or content must be promptly notified to affected users with reasons and redress options.

Article 26. Personal Data Collection

Only personal data strictly necessary for the transaction or account management may be collected, and must never be sold or transferred without consent.

Article 27. Data Security

Operators must use up-to-date encryption and security protocols, and report any data breach or security incident to the Ministry within 72 hours.

Article 28. Data Retention and Deletion

Personal and transactional data must be retained only as long as required by law or contract, and securely deleted thereafter.

PART V. REPORTING, SUPERVISION AND AUDIT

Article 29. Regular Reporting

Quarterly reports on transaction figures, complaints, and compliance incidents must be submitted to the Ministry in prescribed form and detail.

Article 30. Inspection and Audit Powers

The Ministry may conduct periodic or unannounced inspections, including digital audits, requiring full disclosure of books and electronic records.

Article 31. Recordkeeping Standards

Operators must retain complete transaction, complaint, and audit records for at least five years, and provide them upon lawful request.

PART VI. SECTORAL, PUBLIC, AND CROSS-BORDER PROVISIONS

Article 32. Special Sectors

Pharmaceuticals, food, digital assets, and other high-risk sectors are subject to additional, sector-specific licensing and compliance rules.

Article 33. Cross-Border E-Commerce

Operators outside Ethiopia serving Ethiopian consumers must fully comply with this Directive and local consumer and tax law, or risk blocking.

Article 34. VAT and Tax Obligations

Platform operators must register for VAT if providing taxable supplies to Ethiopian users, and ensure all applicable taxes are remitted promptly.

Article 35. Intellectual Property Rights

Operators must promptly remove goods or content upon verified notice of IP infringement by right holders or competent authorities.

Article 36. Notice-and-Takedown

A transparent notice-and-takedown procedure must be in place for illegal or harmful content, with opportunity for counter-notice by affected parties.

Article 37. Public Awareness and Digital Literacy

Operators must provide guidance for users on safe internet use, fraud prevention, privacy, and available consumer protection mechanisms.

PART VII. ENFORCEMENT AND FINAL PROVISIONS

Article 38. Penalties and Sanctions

Violations may result in warnings, fines, suspension, permanent de-listing, and—where criminal activity is involved—referral for prosecution.

Article 38 — Penalties (graded framework)(Revised)

1. Penalties under this Directive shall be graded according to the type and seriousness of the violation and the economic size of the operator.
2. Minor or first-time infringements may result in warnings or small fixed fines, while repeated or serious violations—especially those affecting many consumers—may justify higher, turnover-based fines and, in extreme cases, suspension or revocation

of licenses.

3. A specialized authority, such as the Ethiopian Communications Authority, may be designated to apply this penalty scale, subject to procedural safeguards and judicial review.

Article 39. Appeals and Dispute Resolution

All decisions on licensing, sanction, or removal may be appealed as set out in regulations; an internal dispute mechanism must be maintained and government review available.

Article 40. Transitional Arrangements

Current operators must register and comply with this Directive within a six-month period from the enforcement date; after this period, unlicensed activity will trigger enforcement.

Article 41. Review and Amendment

The Ministry may issue guidance, FAQs, or revisions to address new technologies, market developments, or gaps arising in implementation. A formal review occurs every two years.

Article 42. Entry into Force

This Directive enters into force upon its publication in the Federal Negarit Gazette and shall be binding on all e-commerce activities henceforth.

Strategic Considerations for Ethiopia's E-Commerce and Regional Digital Trade Alignment

4.1. Purpose and Scope of Strategic Considerations

This chapter provides strategic considerations to support the interpretation of the legal and standards-related outputs presented in the preceding chapters. It situates the first-year consultation results within Ethiopia's broader e-commerce development trajectory and the evolving regional digital-trade environment under the AfCFTA framework. By clarifying sequencing considerations, institutional linkages, and structural constraints, this chapter offers a contextual lens through which the standards and legal directives developed during the first year may be understood and assessed. In doing so, it draws attention to key issues relevant to longer-term digital trade alignment and future phases of engagement.

Against this background, Ethiopia's ongoing e-commerce reform efforts—anchored in the National E-Commerce Strategy and the revision of the E-Transaction Proclamation—are examined from an ecosystem perspective. While important progress has been made, e-commerce continues to be framed primarily in platform-centric terms, underscoring the need to move beyond a single-platform view toward a more comprehensive ecosystem approach encompassing payment systems, logistics, authentication, consumer protection, and data management.

In this context, the first-year advisory complements MinT's request for legal and standards-related consultation by mapping Ethiopia's current e-commerce landscape, identifying key stakeholders and institutional structures, and drawing comparative insights from other African countries. These efforts aim to establish a foundation that may inform subsequent phases of consultation, including discussions on integration and expansion strategies.

While the National E-Commerce Strategy identifies relevant policy challenges, it remains largely descriptive, and thus it leaves a gap between diagnosis and

implementation. This advisory seeks to address that gap by introducing an implementation-oriented perspective and proposing ways to translate institutional issues into actionable ecosystem strategies.

Furthermore, the current strategy remains primarily focused on domestic conditions and provides limited reference to regional experiences. Yet, effective implementation of the AfCFTA Digital Trade Protocol would benefit from a comparative review of practices in countries such as Kenya, Rwanda, and South Africa, and from adapting relevant lessons to Ethiopia's context. In this regard, the advisory aims to complement the existing strategy by incorporating regional perspectives and aligning them with international norms.

Finally, although the strategy underscores the need to define e-commerce in an “end-to-end” manner, it offers little guidance on where such an effort should begin. The advisory therefore highlights the national digital ID system (Fayda) as a potential foundation for establishing a trusted authentication framework, which could serve as a practical starting point for developing sequential linkages across payment, logistics, and data-tracking systems.

This document covers four main areas of work.

First, this document builds on the analytical areas already identified in the National E-Commerce Strategy by conducting a preliminary mapping of Ethiopia's e-commerce ecosystem. The mapping focuses on key elements of the value chain—payment infrastructure, logistics and distribution systems, major platforms, and consumer interfaces—while placing particular attention on bottlenecks such as limited payment interoperability, logistical constraints, and weak trust mechanisms including authentication and consumer protection. As this work primarily relies on desk research, the results are intended to complement, rather than replicate, the existing strategy. Further discussions and field-level validation will be required to contextualize and refine the findings.

Second, the document outlines an initial overview of key stakeholders across both public and private sectors. This includes principal government agencies such as the Ministry of Innovation and Technology (MinT), the Ministry of Trade and Regional Integration (MoTRI), the National Bank of Ethiopia (NBE), and the Ethiopian Logistics Commission, along with local startups, logistics and financial companies, small business associations, youth entrepreneurship networks, and international partners such as the AfCFTA Secretariat and the AU Digital Single Market initiative.

Third, the document will undertake a targeted desk review of selected regional experiences, particularly within the AfCFTA context, to benchmark ecosystem approaches and identify structural challenges such as payment interoperability gaps, logistical inefficiencies, and weak trust mechanisms. Drawing on examples from Kenya, Rwanda, and South Africa, the analysis will extract lessons relevant to Ethiopia's institutional and

economic environment. These insights will inform the formulation of policy options that align national priorities with regional digital-trade developments.

Fourth, the document offers an expert observation on a potential entry point for transitioning toward an integrated e-commerce ecosystem. While not part of MinT's initial request, this perspective builds on Ethiopia's ongoing Fayda national digital-ID initiative, which could serve as a foundation for strengthening trust between buyers and sellers. Linking Fayda to e-commerce authentication frameworks would provide a credible basis for interoperability across payment, logistics, and data systems. This suggestion is offered for further discussion and consideration in future advisory phases.

4.2. Analytical Overview and Policy Coherence

4.2.1. Policy Orientation of Ethiopia's Request

At this stage, Ethiopia's current request, as outlined in the draft National E-Commerce Strategy and particularly articulated under Strategic Goal 1, can be understood as reflecting four interrelated policy intentions (See below text box)

Rather than a definitional clarification, these represent a broader policy effort to align national e-commerce regulation with emerging regional digital-trade norms under the AfCFTA.

a. Alignment with Regional Digital-Trade Norms

Ethiopia seeks to revise its E-Transaction Proclamation to include an explicit definition of digital products, thereby achieving coherence with the AfCFTA Protocol on Digital Trade.

The revision process would close the definitional gap that currently excludes digital-only goods and services, such as cloud software, streaming, or online content from the country's trade framework.

b. Comprehensive “End-to-End” Coverage of the E-Commerce Lifecycle

The planned strategy, or revision, broadens Ethiopia's regulatory scope to cover the entire transaction chain; from ordering and payment to delivery, authentication, and consumer protection so that e-commerce is governed as an ecosystem rather than as isolated transactions.

c. Recognition of Multi-Modal Payments and Delivery Channels

Legal acknowledgment of multiple payment and fulfillment methods (including mobile money, card, QR, and cash-on-delivery) reflects an inclusive approach, essential for expanding participation beyond digitally advanced urban areas.

d. Strengthened Regulatory Traceability and Oversight

The inclusion of full-cycle monitoring provisions supports the establishment of traceable transaction data across the value chain, enabling fiscal, customs, and consumer-protection authorities to develop more data-informed oversight mechanisms.

Together, these four directions illustrate Ethiopia's recognition that legal modernization is a prerequisite for ecosystem-level e-commerce governance and cross-border digital-trade integration. In this sense, the proposed revision functions as a conceptual bridge between current domestic regulation and the regional trade architecture envisioned under the AfCFTA Digital Trade Protocol.

The revision of the E-Transaction Proclamation, which aims to expand the legal definition of digital products and align it with the AfCFTA Digital Trade Protocol, is being undertaken within the same advisory framework by a parallel legal team.

In this manuscript, the focus lies on the policy and institutional measures required to translate the revised law into practice—specifically, identifying enabling mechanisms for multi-stakeholder coordination under MinT, advancing interoperability across payment and authentication systems, and strengthening the trust infrastructure necessary for effective ecosystem governance.

From this perspective, the advisory tracks are mutually reinforcing: the legal reform defines the regulatory foundation, while the present analysis informs the ecosystem conditions that will determine its implementation success.

4.2.2. Structural and Governance Constraints Affecting Ethiopia's Alignment with the AfCFTA Digital Trade Protocol

This section examines the structural and political factors that shape Ethiopia's current approach to e-commerce policy implementation, explicitly from the standpoint of policy execution. It first considers the broader, system-level constraints and then turns to the micro-level policy tensions embedded within Ethiopia's current regulatory

and institutional practices. Because this analysis is based on secondary data, these dynamics should be understood as preliminary patterns that require further validation through stakeholder consultations and policy dialogue. Nevertheless, they reveal three key tensions that currently undermine Ethiopia's coherence with the AfCFTA Digital Trade Protocol.

(a) Misalignment Between Domestic Policy Logic and AfCFTA Digital Trade Requirements

Ethiopia's draft National E-Commerce Strategy is shaped by a domestic market-enablement logic, positioning e-commerce as a lever for MSME development, employment generation, and national digital inclusion. This orientation reflects the country's current institutional and infrastructural realities. By contrast, the AfCFTA Digital Trade Protocol is built on a regional harmonization logic, which requires interoperability of trust services, cross-border data governance, multimodal logistics integration, and coordinated regulatory frameworks. These obligations presuppose a level of institutional maturity and cross-agency integration that Ethiopia has not yet fully developed, particularly in payments interoperability, trust services, logistics digitalization, and data governance.

Ethiopia's digital governance architecture is distributed across several regulatory bodies, including the Ministry of Innovation and Technology (MinT), the National Bank of Ethiopia (NBE), the Ethiopian Revenues and Customs Authority (ERCA), the Ministry of Trade and Regional Integration (MoTRI), and the Ethiopian Communications Authority (ECA). While multi-agency governance is common globally, Ethiopia's arrangement remains in an early stage of institutional maturity. No formal mechanism yet exists to harmonize mandates, synchronize regulatory instruments, or define shared responsibilities across agencies. This structural dispersion is directly at odds with the governance logic envisioned in the AfCFTA Digital Trade Protocol, which presupposes integrated national systems capable of supporting cross-border digital trade. For example, Article 19 requires that:

“State Parties shall adopt certification mechanisms and disciplines for the mutual of electronic authentication, digital certificates, digital identities...”

Such mutual recognition mechanisms cannot take shape unless domestic regulators coordinate their respective responsibilities.

In this context, MinT's present emphasis on consolidating the domestic ecosystem is a rational and predictable policy stance rather than an indication of misalignment. Because no single institution is mandated to lead digital trade implementation, agencies default to their existing domains, such as MSME support, domestic platform enablement, cybersecurity, or national digital inclusion. The draft strategy therefore becomes inward-facing by design, not by opposition. The prominence of domestic priorities reflects

structural fragmentation, the absence of a coordinating authority capable of orchestrating regional digital-trade readiness, and the need to establish foundational systems before cross-border interoperability can be meaningfully pursued.

Since no single institution is mandated to lead digital trade alignment, each agency defaults to its existing domain, such as Micro, Small, and Medium Enterprises (MSME), domestic platform enablement, or national digital inclusion. This produces a National E-Commerce Strategy that is inherently inward-oriented. The observed emphasis on domestic markets is therefore not a rejection of AfCFTA's principles but a logical response to fragmented institutional structures and the absence of a coordinating authority capable of advancing regional integration.

This domestic-first posture should thus be interpreted not as a rejection of AfCFTA principles, but as a necessary sequencing choice in a context where the prerequisites for regional integration, including trust architecture, data governance institutions, interoperable digital ID, and multimodal logistics systems, are still under development.

(b) Misaligned Understanding of What Digital Trade Is

A second structural constraint arises not simply from Ethiopia's security-first regulatory posture but from its fundamentally different understanding of what digital trade actually is. The AfCFTA Digital Trade Protocol treats digital trade as an integrated cross-border ecosystem that includes logistics governance, multimodal transport coordination, streamlined licensing procedures, national addressing systems, interoperable trust services, digital identity, and cross-border data mobility. Ethiopia, however, continues to view digital trade primarily as a domestic issue focused on e-transactions, platform oversight, consumer protection, and internal data control. This platform-centric and security-anchored framing directs policymakers toward regulating websites and managing data risks while overlooking the much broader administrative, infrastructural, and governance reforms that the AfCFTA requires. The result is a structural misalignment: Ethiopia's current policy lens treats digital trade as a platform problem, while the AfCFTA frames it as a continent-wide logistics, transport, and governance system that must function seamlessly across borders. This conceptual gap, rather than institutional or technical limitations alone, explains why Ethiopia's implementation remains inward-looking and why meaningful alignment with the AfCFTA requires reframing how digital trade is understood at the national level.

Ethiopia's National Digital Economy Strategy (draft) explicitly recognizes the need to revise the E-Transaction Proclamation to include the definition of digital products and services “to align with emerging trade agreements such as the AfCFTA Digital Trade Protocol.” This demonstrates that Ethiopia's digital legal framework is already oriented toward regional harmonization, acknowledging the Protocol as a reference for defining digital trade and ensuring traceability of e-commerce transactions.

The E-Transaction Proclamation No. 1205/2020 provides the legal framework for electronic communications and signatures but contains no definition of “digital trade,” “digital product,” or “digital service.” Ethiopia's National Digital Economy Strategy (drafted) explicitly recognizes this gap and calls for a revision of the Proclamation “to include the definition of digital products/services to align with emerging trade agreements such as the AfCFTA Digital Trade Protocol.”

At the policy level, it is worth noting that Ethiopia's current legal and strategic frameworks, particularly the Electronic Transaction Proclamation (No. 1205/2020) and the draft National E-Commerce Strategy define e-commerce primarily in terms of digitally enabled transactions of goods and services.

Unlike the AfCFTA Digital Trade Protocol, which differentiates between digital products, digital services, and digitally enabled trade, Ethiopia's definition remains narrowly transactional and does not yet capture the evolving scope of digital-only goods or cross-border service delivery.

This orientation influences decisions related to cloud adoption, data storage, cross-border data transfer, authentication infrastructure, and the management of sensitive government datasets. However, the AfCFTA Digital Trade Protocol adopts a fundamentally different logic that emphasizes openness, interoperability, and cross-border data mobility. Article 20 establishes a clear principle:

“State Parties shall... allow the cross-border transfer of data, including personal data, by electronic means...”

and further stipulates that restrictions must not constitute

“arbitrary or unjustifiable discrimination or a disguised restriction on digital trade.”

Similarly, Article 22 explicitly limits data localization by stating that:

“State Parties shall not require a person of another State Party to use or locate computing facilities in their territories...”

While a security-first orientation is not unique to Ethiopia—indeed, many countries adopt sovereignty-based approaches to data governance—its implications are more structurally constraining in the Ethiopian context. In countries with mature digital governance systems, security-driven rules coexist with counterbalancing mechanisms such as comprehensive personal data protection laws, cloud governance standards, cross-border data transfer frameworks, interoperable digital identity systems, and coordinated multi-agency oversight. Ethiopia has recently taken meaningful steps toward building such mechanisms: the Personal Data Protection Proclamation (No. 1321/2024) establishes a legal framework for data protection, and a presidential decree has created the Government Cloud (G-Cloud) to centralize state information systems for use by

government entities and state-owned organizations. In addition, the Information Network Security Administration (INSA) plays a central role in safeguarding digital infrastructure through cybersecurity mandates and by contributing to the development of emerging data protection frameworks.

However, these initiatives remain primarily inward-facing. G-Cloud is designed for domestic government data hosting rather than providing a national cloud governance framework compatible with cross-border digital trade. Similarly, INSA's mandates focus on cybersecurity and national resilience, leaving significant gaps in interoperability standards, cross-border data transfer rules, and multi-agency coordination. The personal data protection authority is not yet fully operational, and implementing directives for cross-border data governance are still absent. As a result, despite recent legal and institutional progress, Ethiopia's security-first approach continues to narrow the scope of digital policy rather than balance security with interoperability. What is a globally common governance pattern thus becomes, in Ethiopia, an acute structural constraint—one that amplifies the micro-level tension between e-transaction-focused domestic regulation and the broader digital trade ecosystem envisioned under the AfCFTA Digital Trade Protocol.

While AfCFTA defines digital trade broadly, encompassing cross-border digital goods, services, and data exchange, Ethiopia's legal instruments still revolve around domestic transaction-level regulation.

The conceptual terms may appear similar, but the scope of application diverges sharply:

- AfCFTA: cross-border exchange of digital products and services.
- Ethiopia: domestic enablement of digital-platform transactions.

According to the Protocol, “Digital Trade” means digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve natural and juridical persons. This definition anchors the scope of digital trade not merely in the digitization of transactions but in the digitally enabled cross-border exchange of goods and services, whether the delivery itself is digital or physical.

Building on this definition, the Protocol frames digital trade as a system that depends on legal validity of electronic trust services. Article 8 establishes that no State Party may deny the legal effect or admissibility of electronic documents, signatures, seals, timestamps, or other trust services “solely on the basis that they are in electronic form”. Article 9 requires States to maintain laws enabling parties to determine authentication methods and ensure that recognition is not limited by technology type. This demonstrates that AfCFTA views digital trade as inseparable from a trusted digital environment where electronic signatures, documents, and authentication systems are interoperable and mutually recognized.

A close reading of Article 11 of the AfCFTA Protocol on Digital Trade makes it immediately clear that digital trade is not an e-commerce website problem. The Protocol treats digital trade as a comprehensive governance and infrastructural system that extends far beyond online platforms. Article 11 requires State Parties to reform and integrate the entire logistics, transport, regulatory, and addressing ecosystem as a precondition for digital trade.

Article 11(1) obliges State Parties to

“enhance the regulatory environment for logistics services and related freight logistics services... [and ensure] reasonable, transparent, and non-discriminatory” regulation.

This means that digital trade cannot function without logistics governance reform.

Article 11(2) requires States to

“streamline licensing procedures related to logistics services... in a prompt and non-discriminatory manner”.

Here, digital trade is defined not by platforms but by regulatory efficiency in freight and delivery licensing.

Article 11(3) goes further, calling on States to

“promote the establishment of transport coordination mechanisms... improve infrastructure, promote international multimodal transport and interconnectivity... and formulate standard and compatible transport rules”.

This embeds multimodal transport integration directly into the legal definition of digital trade.

Article 11(4) mandates that regulatory decisions affecting logistics service providers be

“impartial, transparent, and non-discriminatory,” and requires States not to adopt measures that “restrain competition”.

Thus, digital trade is defined as a competitive logistics market, not a controlled or state-dominated one.

Finally, Article 11(5) encourages States to

“adopt, maintain or upgrade national addressing systems”,

recognizing that addressing infrastructure is a functional requirement for last-mile delivery, geolocation, routing, and any form of e-commerce or digital services.

Digital Trade as a System

- In AfCFTA's framework, Digital trade is not a “platform economy”; it is an ecosystem and a governance system.
- From the perspective of AfCFTA, digital trade encompasses the entire ecosystem, including:
 - Electronic documentation (Article 10)
 - The regulatory environment for logistics and freight services (Article 11.1)
 - Licensing procedures for logistics operators (Article 11.2)
 - Coordination of multimodal transport and interconnectivity (Article 11.3)
 - A competitive and non-discriminatory logistics market (Article 11.4)
 - A functioning national addressing system (Article 11.5)
- It requires countries to modernize and integrate physical supply chains, regulatory procedures, transport systems, and addressing infrastructure so that cross-border digital commerce can function reliably.
- Thus, Ethiopia's current approach—treating e-commerce primarily as a digital platform issue—fundamentally diverges from the AfCFTA vision, which sees digital trade as a whole-of-economy transformation involving logistics, transport, regulatory coordination, and national infrastructure systems.

(c) Capacity, Timing, and the Institutional Caution Toward Regional Integration

A third structural constraint shaping Ethiopia's digital trade trajectory is the gap between the institutional capabilities required under the AfCFTA Digital Trade Protocol and the domestic systems that Ethiopia is still in the process of building. The Protocol assumes that State Parties can operationalize a wide set of foundational systems, including independent data protection authorities, interoperable digital identity frameworks, cross-border data transfer mechanisms, electronic trust services, multimodal transport coordination, streamlined logistics licensing, and national addressing systems, before engaging fully in regional integration. Because many of these components are either newly established or not yet functional in Ethiopia, institutions have little choice but to take a cautious, incremental approach when interpreting or committing to AfCFTA obligations. This is not reluctance but a structurally rational response to the sequencing and capacity demands embedded in the Protocol itself. Articles such as 42 (technical assistance and capacity building), 43 (cooperation across high-capacity domains), 48 (domestic measures required for implementation), and 37 (institutional arrangements for ongoing coordination) all acknowledge uneven readiness among Member States. These provisions collectively demonstrate that regional digital trade is predicated on extensive

domestic preparation, which explains why Ethiopia's engagement remains deliberately paced and primarily inward-focused as foundational systems continue to emerge.

It is neither possible nor analytically useful to catalogue the full range of technical components involved in a digital-trade trust ecosystem. Beyond PKI, such as authentication protocols, digital identity integration, certificate lifecycle management, timestamping infrastructures, trust lists, secure delivery networks, or electronic document validation, modern digital trade requires dozens of interdependent technical subsystems. Providing a complete technical inventory would shift the focus away from the core objective of this report, which is to assess, from a policy-execution standpoint, whether Ethiopia currently possesses the foundational institutional, governance, and operational capacities that AfCFTA implementation presupposes.

Nevertheless, it remains important to identify a minimal set of technical elements so that policymakers can accurately understand the structural dependencies that shape Ethiopia's digital-trade readiness. To support this, the report provides a concise table summarizing only the essential technical components—sufficient to inform policy considerations, without expanding into an exhaustive technical inventory.

Capacity Building as a Precondition, not a Supplement

Article 42 states that State Parties “agree to support and strengthen the capacity... to enable and promote digital trade” and to “facilitate the implementation” of the Protocol. This clause explicitly acknowledges that digital trade implementation requires administrative, technical, and regulatory capacities that many Member States, particularly low-income or institutionally consolidating economies do not yet possess. AfCFTA therefore embeds capacity development as a structural element of digital trade, not as an optional add-on.

Ethiopia is still constructing foundational systems; including 1) Data Protection Authority (post-2024 law) 2) an interoperable national digital identity (Fayda/NIDP) 3) digital logistics and multimodal transport coordination 4) electronic trust service frameworks,¹⁵ 5) digitized customs and e-document workflows.

Institutions cannot commit to cross-border digital trade without first ensuring that domestic systems can enforce, monitor, and maintain them. Article 42 essentially validates this sequencing.

¹⁵ Article 8 — Electronic Trust Services explicitly include electronic signatures, electronic seals, electronic timestamps, registered electronic delivery services, and other forms of electronic trust services. Article 9 — Electronic Authentication explicitly refers to: Authentication methods chosen by parties, Recognition of authentication technologies, Proof of validity before authorities, no limitation on accepted authentication models, and technology-neutral recognition. Article 19 — Interoperability and Mutual Recognition explicitly include: Electronic authentication, digital certificates, digital identities, electronic timestamps, electronic invoices, electronic signatures, and other mutually recognizable electronic trust elements.

Implementation Requires External Technical Support

The Secretariat must “coordinate the provision of technical assistance and capacity building” to help States implement the Protocol (Article 42(2)). This clause shows that AfCFTA does not assume uniform readiness; implementation is expected to be incremental and externally supported. It formalizes sequenced integration as part of the treaty design.

Institutions become cautions because they understand that reforms required external coordination, multi-agency cooperation, and new technical competencies. Ethiopia's institutions, including MinT, INSA, ERCA, Customs Commission, NIDP, and sectoral regulators must sequence reforms across multiple domains. Without coordinated assistance, simultaneous alignment on digital identity, logistics regulation, e-documentation, and cross-border data flows is unrealistic.

Cooperation Across High-Capacity Domains

Article 43 lists cooperation areas: personal data protection, cross-border data transfer mechanisms, authentication, digital identity, logistics, electronic invoicing, interoperability, digital payments, infrastructure, and more.¹⁶

Article 43 effectively outlines the institutional architecture of digital trade. Each areas requires specialized agencies, legal frameworks, technical standards, auditing mechanisms, and cross border agreements.

Nearly every system listed in Article 43 is still in early development in Ethiopia. The country is a) launching Fayda ID but not yet integrating authentication systems b) establishing a DPA but with limited operational capacity c) modernizing logistics but lacking multimodal transportation integration d) digitalizing customs but still paper-based in key flows, and e) exploring cross-border data flows but without legal mechanisms.

Domestic Measures Required Prior to Implementation

Article 49 requires that State parties “apply appropriate measures to bring into effect the rules and procedures set out in this Protocol.” This clause makes it explicit that countries cannot implement AfCFTA digital trade rules unless the necessary domestic

¹⁶ a. protection of personal data; b. cross-border data transfers; c. online consumer protection; d. cybersecurity; e. unsolicited commercial electronic communications; f. electronic authentication; g. electronic signatures; h. digital payments; i. electronic invoicing; j. logistics; k. digital identities; l. electronic transferable records; m. digital inclusion; n. micro, small and medium-sized enterprises; o. digital skills development; p. digital innovation and entrepreneurship; q. emerging and advanced technologies; r. financial technology; s. data innovation; t. interoperability and mutual recognition; u. online safety and security; v. open government information; w. anti-money laundering and combatting the financing of terrorism x. digital infrastructure; and y. any other areas relevant to boost, facilitate and regulate digital trade

systems already exist. Implementation is not a legal declaration but an operational process that depends on functioning institutions, technical infrastructure, administrative mechanisms, and coordinated regulatory frameworks.

Article 48 is deceptively short, but it is one of the strongest and most demanding provisions in the AfCFTA Digital Trade Protocol. It states that each State Party must “apply appropriate measures to bring into effect” the Protocol's rules and procedures. For Ethiopia, the domestic prerequisites implied by Article 48 remain largely underdeveloped. Bringing AfCFTA obligations into effect requires a baseline of systems that Ethiopia is still building, which means that immediate compliance with AfCFTA's digital trade requirements is not practically achievable.

At the institutional level, Ethiopia lacks several of the core governance structures that Article 48 implicitly assumes. The 2024 Personal Data Protection Proclamation has been enacted, but the Data Protection Authority, the central institution needed to regulate cross-border data flows, conduct adequacy assessments, certify processors, and enforce compliance, has not yet been established. The country also does not have a functioning national trust service framework, despite AfCFTA Articles 8, 9, and 19 requiring capabilities such as electronic signatures, electronic seals, timestamps, registered electronic delivery, digital certificates, and the mutual recognition of digital identities. Ethiopia has no operational Public Key Infrastructure (PKI), no trust service providers, no certificate policies, no revocation systems, and no mechanisms to negotiate cross-border trust agreements; all of which are prerequisites for implementing AfCFTA's trust-service chapters. Likewise, multimodal logistics regulation remains fragmented across separate regulators for road, rail, aviation, maritime transport, and last-mile delivery. Ethiopia has no coherent transport coordination mechanism, even though Article 11(3) explicitly requires one.

At the technical level, the gaps are equally significant. Ethiopia does not yet have an operational Public Key Infrastructure (PKI) or digital certificate infrastructure; electronic identity (Fayda) remains in rollout and is not integrated with authentication or e-signature technologies; electronic documents are not recognized or exchanged across borders; and there is no national addressing system, which is essential for routing, e-invoicing, trade documentation, and last-mile delivery. None of the core technical elements required by Articles 8, 9, 10, 11, or 19 are currently available in functional form. Without these foundational systems, Ethiopia cannot implement electronic trust services, electronic authentication, or the mutual recognition obligations that sit at the center of AfCFTA's digital trade architecture.

At the operational level, Ethiopia does not yet possess the day-to-day mechanisms required to enforce or monitor AfCFTA compliance. The country lacks cross-border data transfer rules (Article 20), interoperable e-documentation for customs and SPS processes (Article 10), competitive logistics regulation (Article 11), and any form of electronic trust-

service recognition (Article 19). These are not administrative refinements but deep operational capabilities that must be built before the Protocol's provisions can take effect.

However, it is important to note that these constraints are not unique to Ethiopia. Many Sub-Saharan African countries face similar gaps in trust services, digital identity integration, data governance, logistics coordination, and electronic documentation. This is precisely why the AfCFTA Digital Trade Protocol explicitly emphasizes capacity building (Article 42) and cooperation across high-capacity domains (Article 43): the Protocol's drafters recognized that a significant number of Member States lack the institutional and technical foundations needed for immediate implementation. Ethiopia's situation therefore reflects a broader regional pattern, not an exception, underscoring the centrality of capacity development as a prerequisite for meaningful digital trade integration in the continent.

Table 4-1 Minimum Technical and Institutional Components for AfCFTA Digital Trade Readiness

AfCFTA Requirement	Relevant Articles	Meaning / Nature of the System	Ethiopia's Current Status	Implication for Capacity & Timing
National Digital ID	Art. 19 (Mutual Recognition), Art. 9 (Authentication)	Interoperable digital identity enabling verification across borders	Fayda ID expanding; no interoperability or trust linkage yet	Multi-year work on identity federation, trust anchors, and authentication standards
Data Protection Authority	Art. 21 (Data Protection), Art. 43 (High-Capacity Domains)	Independent authority for data governance, adequacy decisions, and cross-border compliance	2024 law enacted; DPA not yet operationalized	Delays ability to adopt cross-border data flow commitments
Cross-border Data Transfer Mechanisms	Art. 20 (Data Flows)	Default allowance with regulated exceptions; requires adequacy, safeguards, and governance	No operational mechanism; security-first regulatory posture	Requires new regulations, safeguards, and institutional trust frameworks
Interoperable Trust Services	Art. 8, 9, 19	Electronic signatures; electronic seals; timestamps; registered e-delivery; authentication methods; digital certificates; digital IDs; e-invoices; mutual recognition of trust services	Domestic trust services minimal; no cross-border recognition; PKI not operational at scale	Major legal and technical capacity gap; multi-year PKI and trust architecture development needed

AfCFTA Requirement	Relevant Articles	Meaning / Nature of the System	Ethiopia's Current Status	Implication for Capacity & Timing
Multimodal Transport Integration	Art. 11(3)	Integrated regulation of road–rail–air–maritime + regional coordination	Fragmented regulators; limited multimodal interoperability	Structural constraint on regional digital logistics
Digital Logistics Market	Art. 11(1), 11(4)	Transparent, competitive logistics and delivery services	Highly fragmented, informal, and restrictive market	Limits modernization of e-commerce and supply chain efficiency
Streamlined Licensing	Art. 11(2)	Efficient, non-discriminatory logistics licensing and permitting	Licensing complex; multiple agencies; slow cycles	Administrative bottlenecks hinder compliance and implementation speed
E-document Workflows	Art. 10	Legal equivalence and regional usability of e-documents (customs, SPS, permits)	Customs & SPS remain predominantly paper-based	Requires digitization, legal reform, and system integration
National Addressing System	Art. 11(5)	Core infrastructure for routing, delivery confirmation, and last-mile logistics	Addressing system incomplete and unevenly implemented	Fundamental gap for logistics, delivery, and cross-border e-commerce

4.3. Stakeholder Landscape Overview for AfCFTA Digital Trade Implementation in Ethiopia

This section maps the key public, semi-public, and private actors whose mandates directly affect Ethiopia's ability to align with the AfCFTA Digital Trade Protocol. The objective is not to generate an exhaustive list of institutions, but to identify which entities hold decision-making, regulatory, operational, or infrastructural authority over the systems required by Articles 8, 9, 10, 11, 19, 20, 21, and 48.

4.3.1. MinT's Legally Defined Mandate and Alignment with AfCFTA

Under its establishment proclamation (Proclamation No. 1263/2011, Article 29), the Ministry of Innovation and Technology (MinT) is legally entrusted with a broad and strategic mandate that positions it as Ethiopia's national authority for digital transformation. The law assigns MinT the following core functions:

- Policy Initiation and Strategic Planning
 - Initiate national policies, strategic, laws, and programs for digital economic development.
 - Prepare detailed national programs aligned with Ethiopia's overall development plan.
- Digital Innovation and Technology Governance
 - Formulate and implement national innovation, technology, and digital R&D strategies.
 - Coordinate national research programs and identify emerging digital technology areas.
- Cross-Sector Coordination
 - Work in collaboration with concerned organs to align curricula, information systems, digital infrastructure, and innovation programs.
 - Provide technical and professional support to federal and regional institutions.
- Regulatory Standards and Digital Infrastructure Modernization
 - Set national standards, together with relevant organs, to ensure the quality, security, and reliability of ICT services.
 - Monitor the implementation of these standards across sectors.
 - Organize national innovation and technology databased and oversee information management standards.
- Support to Digital Ecosystem Development
 - Promote private-sector participation in digital innovation.

- Facilitate digital infrastructure expansion and ensure public services are supported by appropriate technology.
- Strengthen secured information networks across government institutions.
- Knowledge Systems and Technology Transfer
 - Register, preserve, and disseminate technological information.
 - Support indigenous technology development, prototyping, and commercialization.

These roles demonstrate that MinT is not an operational agency for digital services, but rather Ethiopia's strategic authority for digital governance, standard-setting, and ecosystem coordination.

These statutory functions make MinT the logical national counterpart for AfCFTA Digital Trade Protocol alignment, even though many of the operational functions required for implementation—digital ID, PKI, payments, logistics, data protection—lie outside its direct control.

Table 4-2 MinT Mandate based Digital Trade Mapping Table

MinT Legal Mandate (Proclamation No. 1263/2021)	Legal Basis (Exact Clause)	Digital Trade Relevance (AfCFTA)	Related AfCFTA Articles
1. National digital policy & strategy initiation	“initiate policies, strategies, laws and programs for... digital economic development”	Digital trade requires national policy frameworks, digital economy strategy, and alignment with regional protocols	Art. 48 (Domestic institutional arrangements)
2. Strategic planning aligned with national development plan	“prepare a detailed program... compatible with national development plan”	Digital trade implementation requires national roadmap, sequencing, and cross-sector integration	Art. 48; Art. 10–11 (implementation readiness)
3. Digital innovation & technology governance	“prepare and implement national innovation and technology R&D policies, strategies, and programs”	Supports digital trade innovation, standards adoption, DPI readiness, and technology governance	Art. 19 (trust services); Art. 20–21 (data governance)
4. Cross-sectoral coordination with concerned organs	“in collaboration with concerned organs...” (multiple clauses)	Digital trade spans logistics, ID, payments, customs, data — MinT is the only legal cross-sector coordinator	Art. 11 (logistics); Art. 10 (e-documents); Art. 19 (interoperability)

MinT Legal Mandate (Proclamation No. 1263/2021)	Legal Basis (Exact Clause)	Digital Trade Relevance (AfCFTA)	Related AfCFTA Articles
5. Standard-setting for ICT quality, reliability, and security	“set... standards to ensure quality, reliability and security of ICT services; monitor implementation”	Directly relevant: electronic signatures, authentication, cybersecurity, trust services, e-documents	Art. 8 (e-signatures); Art. 9 (authentication); Art. 19 (mutual recognition)
6. National information management standards	“organize innovation and technology databases... set national standards for information management”	Core for cross-border data flows, adequacy, safeguards, data integrity	Art. 20 (cross- border data transfers); Art. 21 (personal data protection)
7. Digital infrastructure modernization for public services	“ensure critical public systems are supported by appropriate technology”	Digital trade requires interoperable national digital identity, payments, logistics, DPI systems	Art. 11 (logistics); Art. 19 (digital ID); Art. 10 (e-docs)
8. Coordination of secure information systems across government	“support the development and coordination of information systems; provide secured information networks”	Relevant to authentication, PKI, cybersecurity, and national trust frameworks	Art. 8–9 (trust/ authentication)
9. Promotion of private-sector participation	“establish a system... for participation of the private sector”	Digital trade ecosystem requires e-commerce platforms, logistics operators, fintech, data processors	Art. 11(4) (competition; non- discrimination)
10. Support for innovation, technology transfer, and indigenous technology	“support studies, research... make prototypes accessible”	Helps local digital trade actors, SMEs, and startups integrate into AfCFTA regional markets	Art. 11; Art. 48 (institutional/ enabling environment)

4.3.2. MinT's Stakeholder Landscape Overview

This observation aligns with the draft Ethiopia National E-commerce Strategy, which identifies as its principal objective “building a thriving and competitive e-commerce market locally and globally.” The draft strategy explicitly recognizes that such a goal requires an ecosystem-level approach, rather than a single-platform solution. It states that “the e-commerce system will be supported by interconnected elements comprising buyers and

sellers enabled by diverse payment systems and supported by extensive logistics and delivery systems.” It further adds that “underlying components will include various digital platforms, with the government providing enabling policies and regulations.”

However, while the strategy acknowledges the need for such ecosystemic approach, the current institutional reality remains fragmented. At this stage, the objective is not to produce an exhaustive mapping but to present a baseline landscape reflecting the institutional configuration as currently understood. However, the boundaries of coordination, particularly between MinT and MoTRI remain unclear, and mechanisms for structured engagement of non-state actors are not yet defined. This implies that MinT’s current coordination role is largely symbolic, centered on convening discussions rather than exercising sustained governance authority. Further clarification of institutional responsibilities and stakeholder participation frameworks will therefore be required in subsequent advisory phases.

This analysis is based on Strategic Goal 1 of the Ethiopia National E-Commerce Strategy (draft). While the draft strategy articulates a clear vision for an integrated e-commerce ecosystem, its strategic goals and institutional assignments reveal overlapping mandates and fragmented responsibilities across government agencies. Certain functions, such as digital-payment regulation, logistics facilitation, consumer protection, and data governance, are distributed among multiple entities without a clear coordination mechanism. In some areas, responsibilities are duplicated or ambiguously defined, while in others, critical components (e.g., digital-identity integration, interoperability standards, and trust infrastructure) are under-represented or omitted.

In particular, the role of the Ministry of Innovation and Technology (MinT) —officially designated as the coordinating body for digital transformation, which appears broad but insufficiently operationalized. MinT is positioned as both a policymaker and a facilitator, yet lacks an institutionalized mechanism to steer inter-ministerial coordination or to ensure private-sector participation in ecosystem development. This ambiguity constrains the implementation of the ecosystem approach envisioned in the strategy and underscores the need for a coherent governance framework that defines clear roles, sequencing, and accountability mechanisms among MinT, NBE, NIDP, and other sectoral agencies.

(a) Ambiguity of MinT's Role: Broad Mandate without Operational Mechanisms

MinT is listed as lead or co-lead in numerous activities, including as the revision of the E-Transaction Proclamation (1.1.1), development of the Consumer Protection and Data Protection Proclamations (1.1.10 & 1.1.11), establishment of a National Cloud Policy (1.1.16), and creation of IoT standards (1.1.19). However, despite its broad leadership designation, the means of exercising coordination authority are undefined. It should be acknowledged that the National E-Commerce Strategy is still in draft form, and therefore may not yet aim to articulate detailed operational procedures or fully codified

institutional mechanisms. The absence of a formalized secretariat, joint KPI framework, or budgetary coordination may partly reflect the draft's strategic level orientation, rather than oversight. Nevertheless, even at this conceptual stage, the lack of an indicative coordination model introduces uncertainty regarding how inter-ministerial collaboration will be institutionalized, and whether MinT's broad mandate can defectively translate into execution capacity.

At the current draft stage, no single institution is explicitly tasked with operational responsibility for implementing e-commerce frameworks. The structure remains policy-heavy and coordination-light, relying on MinT's leadership without defining which entity executes or maintains digital infrastructure. [Table 4-3] summarizes inferred operational responsibility by function at the draft stage. This ambiguity leaves the operational dimension; particularly around trust services (payments, identity, data), undefined, which will need to be clarified in the next phase of strategy finalization or through a dedicated implementation framework annex.

A close reading of Ethiopia's Digital Strategy Draft reveals a fragmented allocation of mandates with significant gaps in operational responsibility. While MinT is positioned as the policy lead, execution functions across payments (NBE), logistics (MoTL, ECC), data governance (INSA, MoJ), and digital identity (NIDP/Fayda) are either missing or insufficiently defined. The omission of critical actors such as the National ID Program and the Data Protection Authority indicates that the strategy does not yet incorporate the institutional ecosystem required for implementing AfCFTA's digital trade obligations. The result is a structural misalignment: the draft provides vision, but not the operational governance architecture needed to execute it.

**Table 4-3 Inferred Operational Responsibility Structure
(Based on the Draft Ethiopia National E-Commerce Strategy)**

Function	Potential Operational Actor	Status in Draft	Comment
Policy design / coordination	MinT	Mentioned as Lead	Policy-level only, no execution tool
Payments	NBE	Not clearly assigned	Major operational gap
Trade & logistics	ECC, MoTRI	Co-lead	Partial, lacks measurable tasks
Consumer protection	ECA	Partner	Enforcement implied but not formalized
Data governance	INSA / MoJ	Partner	Technical oversight, unclear scope
Digital identity (authentication)	NIDP (Fayda)	Not included	Critical omission

Source Author's analysis based on the draft strategy (MinT)

MinT is the central policy institution for Ethiopia's digital transformation, yet most of the operational systems required by the AfCFTA Digital Trade Protocol, including trust services, digital identity, payments, multimodal logistics, customs documentation, data governance, lie outside MinT's direct authority. This structural distribution of mandates makes MinT's role primarily architectural and coordinative rather than operational. As a result, effective AfCFTA alignment will depend not on MinT acting alone, but on MinT's ability to orchestrate a multi-agency implementation framework across NIDP, INSA, NBE, MoTRI, MoTL, ERCA, and the forthcoming Data Protection Authority.

(b) Overlap and Imbalance among Institutions

[Table 4-4] summarizes functional overlaps and gaps across agencies found in the draft stage of National E-Commerce Strategy. For instance, while the National Bank of Ethiopia (NBE) is institutionally responsible for payment regulation and digital finance oversight, the draft strategy rarely identifies NBE as a lead agency. It is mentioned only as a supporting partner under the Computer Crimes Proclamation (1.1.8), leaving the operational regulation of digital payments largely unassigned.

Table 4-4 Functional Overlaps and Gasp across Agencies (Draft Stage)

Functional Area	Observation	Explanation
Trade & Customs (MoTRI, ECC, MoF)	Overlapping mandates	Activities 1.1.2–1.1.6 assign all three institutions concurrent leadership for registration, valuation, and clearance—creating accountability diffusion.
Consumer & Data Protection (MinT, MoJ, ECA)	Role ambiguity	MinT is lead for 1.1.10–1.1.11, but the enforcement authorities (ECA, MoJ) are not formally defined.
Digital Payments (NBE, MoF)	Regulatory gap	Only 1.1.8 (Computer Crimes Proclamation) references payments indirectly; no clear mandate for payment interoperability or oversight by the National Bank of Ethiopia.
Digital Identity (NIDP/Fayda)	Complete omission	The authentication layer that is essential for trust and consumer protection is absent from Strategic Goal 1.

Source Author's analysis based on draft strategy (MinT)

Similarly, in the area of trade logistics and cross-border data management, both the Ministry of Trade and Regional Integration (MoTRI) and the Ethiopian Customs Commission (ECC) Are listed as co-leads for activities such as cross-border harmonization, valuation, and risk management (1.1.4 & 1.1.6). This suggests that ECC may hold practical responsibility for operational facilitation, yet no explicit operationalization framework or performance indicator is defined.

In terms of consumer protection and data governance, the Consumer Protection task (1.1.10) assigns MinT as lead with the Ethiopian Consumer Authority (ECA) as partner, and the Data Protection task (1.1.11) lists MinT as lead and the Ministry of Justice (MoJ) as partner. Hence, while ECA and MoJ are expected to carry enforcement functions, the draft offers no explicit operational mandate for these entities. The Information Network Security Agency (INSA) is also mentioned in connection with data security and cybercrime, but only in a technical capacity, without a defined institutional enforcement role.

Finally, digital identity and authentication that is a critical trust component for e-commerce are entirely absent from Strategic Goals 1–3. Neither the National ID Program (NIDP) nor the Fayda ID system appears among the listed stakeholders, leaving a major gap in the strategy’s operational architecture. This omission should be addressed explicitly in future revisions, as it limits the integration of authentication, Know Your Customer (KYC), and consumer-trust mechanisms across Ethiopia’s digital-commerce ecosystem.

(c) Coordination Mechanism: Nominal but weak in Practice

The draft instructs that a National E-Commerce Group¹⁷ be established “with representatives from the public and private sectors.” MinT is designated as Lead with MoTRI (Co-Lead), and the activity is listed under Strategic Goal 1: Establish E-commerce Policy and Regulatory Best Practices and Oversight. However, the draft provides no further detail on the group’s composition, legal status, budgetary arrangements, decision making authority, or reporting structure.

While MinT and MoTRI share nominal leadership, their institutional mandates and bureaucratic affiliations differ fundamentally. From our understanding, MinT operates under the national digital transformation agenda, reporting to the Prime Minister’s Office and focusing on innovation, ICT, and digital economy. MoTRI, on the other hand, governs trade policy, export facilitation, and regional market integration under the economic affairs clusters.

This dual-lead configuration introduces structural ambiguity. Each ministry operates separate budget lines. (At this point), no cross-ministerial KPI framework identified. Neither entity holds statutory superiority. Moreover, dual clearance required for every action item. This co-lead model, while inclusive, however, can dilute ownership and accountability. Without a clear secretariat structure or hierarchy, MinT leadership remains symbolic rather than functional.

¹⁷ Concept of National E-Commerce Group is introduced in this chapter, however, its specified roles and responsibilities across ministries or relevant sectors can be completed after cross-check many other...

Based on the Draft National E-Commerce Strategy and available institutional mandates, our current understanding is as follows:

MoTRI (Ministry of Trade and Regional Integration) is identified as a Co-Lead or Partners in several activities under Strategic Goal 1 particularly those related to customs harmonization, cross-border trade, valuation and taxation. This indicates its responsibility for the trade and market-regulation of e-commerce, including export/import procedures and trade data oversight. However, MoTRI's mandate does not extend to the coordination of digital infrastructure or trust systems, including payments, digital identity, data governance, or consumer protection. These domains remain distributed among MinT, NBE, INSA, ECA, and other agencies.

Consequently, at this stage, it is reasonable to consider MoTRI as the primary focal institution for trade-related operations, while recognizing that ecosystem-level coordination, including linking payments, logistics, data, and authentication, remains institutionally unassigned. This interpretation reflects our current analytical understanding, based on the draft strategy and existing policy frameworks.

It does not imply a formal institutional designation, but rather highlights the present functional gap that future advisory work—particularly in the second-year phase—should revisit and clarify.

In addition, mechanisms for inclusion of public and private sector actors require further elaboration. This lack of clarity weakens both accountability and stakeholder trust, undermining one of the state purposes of the Group: to establish a credible and inclusive coordination framework.

Given these uncertainties, this advisory does not assume that MinT will immediately act as an empowered regulator or ecosystem integrator. Instead, it identifies the potential institutional pathways that could be explored once the ministry's internal priorities, legal authorities, and coordination mechanisms become clearer.

The Draft Ethiopia National E-Commerce Strategy positions MinT as a wide-ranging policy leader, but omits the operational architecture required to implement AfCFTA-aligned digital trade (See [Table 4-5]). Payments (NBE), digital identity (NIDP/Fayda), data protection (MoJ/DPA), logistics and customs (MoTRI/ECC), and cybersecurity (INSA) are outside MinT's control yet are not formally assigned. This produces a structural gap in which MinT is responsible for digital trade strategy but lacks the instruments to execute it. A multi-agency implementation model must therefore be articulated in the next stage of policy design.

Table 4-5 MinT Actual Execution Gap (Based on the Digital Economy Strategy)

Dimension	What MinT Is Assigned (Draft Strategy/ Proclamation)	What Is Operationally Required (AfCFTA)	Who Actually Controls It	Gap Identified
Policy & Strategy Design	MinT listed as Lead in E-Transaction, Consumer Protection, Data Protection, Cloud Policy, IoT Standards	National digital trade strategy; AfCFTA alignment (Art. 48)	MinT	Authority exists, but execution tools absent.
Payments	Mentioned only indirectly (Computer Crimes Proclamation 1.1.8)	Payment interoperability, digital finance regulation	NBE	Major operational gap; NBE missing from strategy.
Digital Identity/ Authentication	Not mentioned at all	Cross-border authentication; e-signatures; digital identity (Art. 8, 9, 19)	NIDP / Fayda	Critical omission; trust system cannot function.
Data Governance/ Protection	MinT Lead; MoJ Partner for Proclamations	Cross-border transfers (Art. 20–21), DPA establishment	MoJ / INSA / DPA (future)	Oversight unclear; enforcement missing.
Logistics & Trade Facilitation	MoTRI + ECC as Co-Leads in valuation, harmonization	Logistics transparency (Art. 11), multimodal transport, addressing systems	MoTRI, ECC, MoTL	Mandates overlap; no operational KPIs.
Consumer Protection	MinT Lead; ECA Partner	Enforcement mechanisms; dispute resolution (Art. 14–16)	ECA	MinT leads policy, but ECA enforcement undefined.
Customs & SPS	ECC, MoTRI referenced; roles not defined	E-documents; e-certification; customs data flows (Art. 10)	ECC / MoA	Operational authority not linked to strategy.
Cybersecurity/ PKI	INSA mentioned indirectly	PKI trust services; root certificates (Art. 8–9)	INSA	Technical role recognized, but no governance model.

4.4. Comparative Insights from Regional Experiences

This section primarily examines selected African countries to illustrate diverse trajectories of e-commerce development across the continent. While Ethiopia's National E-Commerce Strategy frequently references advanced economies, including Korea, as benchmarks, such examples reflect structural conditions that differ significantly from Africa's current stage of digital transformation. Korea's experience, for instance, demonstrates early institutionalization: the launch of Interpark in 1996 and the enactment of the Framework Act on Electronic Transactions in 1999 positioned the country as one of the first movers in global e-commerce. However, this trajectory was driven by advanced infrastructure, high internet penetration, and a digitally literate consumer base—factors that make direct comparison with African contexts less meaningful. Therefore, the following discussion turns to selected African cases that offer more contextually relevant insights into platform development, regulatory evolution, and ecosystem readiness.

In this advisory, three African countries are selected for regional benchmarking: South Africa, Kenya, and Rwanda. Among African states, South Africa scored 56.5 on the UNCTAD B2C E-Commerce Index (2020), representing one of the most advanced contexts on the continent in terms of trust infrastructure, logistics, and overall readiness. Kenya, which scored 49.0 and ranked 88th globally, was chosen for its leadership in mobile-based payments and financial inclusion, offering lessons on interoperability and user adoption. Rwanda is highlighted for its proactive digital-transformation policies and institutional integration efforts, although its 2020 index score is not publicly available; the most recent reference, from 2018, recorded 32.7. Ghana is included in the regional comparison due to its strong record in trade-facilitation digitalization, especially in customs, ports, and logistics systems. Ghana scored 43.8 on the UNCTAD B2C E-commerce Index(2020), ranking 102nd globally, which is higher than many western African countries.

Together, these four countries illustrate complementary dimensions within Africa's emerging e-commerce ecosystem: trust, payments, scale, and institutional readiness, providing evidence-based insights relevant to Ethiopia's ongoing transition. The selection is grounded in measurable indicators rather than anecdotal choice, ensuring analytical comparability with the objectives of Ethiopia's National E-Commerce Strategy and its alignment with the AfCFTA Digital Trade Protocol.

Particularly, this section examines how four African economies, including Rwanda, Kenya, Ghana, and South Africa have approached structural and sequencing challenges similar to those Ethiopia is beginning to encounter in the early stages of its e-commerce policy implementation. Rather than proposing reform models or prescribing specific pathways, the comparison highlights the diversity of approaches taken across the region and illustrates the different ways countries have navigated issues of institutional

coordination, legal development, and digital-trade readiness under varying constraints.

Given Ethiopia's pre-ratification status and its focus on domestic ecosystem consolidation, this section interprets the AfCFTA Digital Trade Protocol not as an immediate compliance framework but as a long-term reference horizon guiding the step-by-step development of national digital-economy institutions.

While several African countries have built strong platform-based digital ecosystems, these primarily facilitate domestic e-transactions rather than cross-border digital trade. The distinction is critical: digital trade implies integration into regional or global value chains through cross-border delivery of digital goods, services, or data.¹⁸

Globally, only a handful of economies, such as Singapore, Korea, and the United Kingdom, currently conduct measurable digital trade, characterized by cross-border delivery of digital goods, services, and data. In Africa, countries like South Africa and Kenya have begun this transition by formalizing digital service taxation and ICT service exports, though regional interoperability remains nascent. Kenya and Rwanda have achieved significant progress in digitizing commerce and services domestically; however, evidence of sustained cross-border digital-trade flows remains limited. Ethiopia, by contrast, remains in the e-transaction phase, where digitalization supports domestic market efficiency rather than cross-border trade flows.

Across Africa, no country has yet fully transitioned into the “Digital Trade Layer” envisioned under the AfCFTA Digital Trade Protocol—defined by cross-border trust services, interoperable digital identity, regulated data mobility, mutually recognized electronic documents, and integrated multimodal logistics. Instead, countries display partial and fragmented progress: Rwanda demonstrates the strongest domestic digital-government integration through RISA, NIDA, and IreboGov, yet its systems remain nationally bounded with minimal regional extension; Kenya exhibits the most explicit strategic intent toward cross-border digital commerce, supported by fintech-led regional transactions, but lacks the legal, regulatory, and trust-service infrastructure required for interoperable digital trade; South Africa possesses the continent's most mature digital-economy legal architecture (ECTA, POPIA, Cybercrimes Act) and advanced technical capabilities, but its orientation remains domestically focused, with no cross-border digital-trade framing or operational mechanisms; Ghana excels in port and customs digitalization through ICUMS and the paperless port program, but this represents

¹⁸ Digital trade becomes operational only when e-transactions evolve into cross-border exchanges of digitally deliverable goods, services, or data. According to the WTO, UNCTAD, and OECD, this transition requires four enabling conditions: (1) a regulatory framework that recognizes digital trade in national or regional trade law; (2) infrastructure for cross-border data flows and digital service delivery; (3) measurable exports of digitally deliverable services recorded in national or international statistics; and (4) participation in international digital-trade or e-commerce agreements (e.g., DEPA, AfCFTA Digital Trade Protocol, CPTPP). Countries lacking these combined features may demonstrate digitalization of commerce but not yet operational digital trade.

modernization of physical trade rather than a transition to the higher-order digital-trade ecosystem involving data, services, trust frameworks, and interoperability. In short, African progress is domain-specific and incomplete, meaning Ethiopia is not catching up from behind a fully established regional benchmark but entering a field in which all peers are still in early stages—creating a strategic opportunity to shape first-generation alignment with the AfCFTA Digital Trade Protocol.

[Table 4-6] summarizes the distinct pathways these countries have taken, highlighting how each has sequenced its digitalization efforts under different institutional and policy constraints. Together the four regional comparators reveal that no African country has fully operationalized digital trade as defined by the AfCFTA Digital Trade Protocol. Kenya leads in strategic ambition but lacks institutional depth; Ghana excels in trade-facilitation digitalization but remains outside the higher digital trade layer; Rwanda offers the continent's strongest domestic digital public infrastructure ecosystem but does not frame digitalization as cross-border trade. Ethiopia's position, that is foundational, domestic-first, and institution-building aligns with patterns observed across the continent, suggesting that a phased domestic consolidation to regional interoperability pathway is both realistic and strategically coherent.

Ghana as one of Africa's most advanced countries in electronic customs processing, risk management, and paperless port operations. While Ghana's progress has been concentrated in the logistics and trade-facilitation layer rather than in cross-border data governance, trust services, or digital-services exports, its experience offers relevant insights for Ethiopia on sequencing reforms and strengthening the “logistics backbone” needed for future digital-trade readiness.

Rwanda has built one of Africa's most coherent digital public infrastructure ecosystems, supported by National Identification Agency (NIDA), Rwanda Information Society Authority (RISA), and a tightly integrated gov-tech architecture. Its domestic systems, including digital ID, PKI, data governance, and e-government are among the continents' most advanced. However, Rwanda does not explicitly frame its digital transformation as a regional trade agenda, and cross-border interoperability (data flows, digital-ID recognition, trust-service mutual recognition) remains underdeveloped.¹⁹

South Africa's possesses Africa's most advanced digital regulatory environment,

¹⁹ Globally, only a very small number of regions have advanced cross-border digital identity and trust-service interoperability. The European Union's eIDAS framework is the closest to a full-scale model-covering electronic signatures, seals, timestamps, electronic delivery, and the mutual recognition of national eOIDs. Even so, EU member states' digital IDs are not fully interoperable, and actual cross-border usage remains uneven and relatively low. Outside the EU, examples exist only in limited or pilot forms: Nordic cooperation through bank-based digital IDs, partial interoperability efforts within the GCC (<https://www.norden.org/en/declaration/declaration-nordic-and-baltic-ministers-digitalisation-promoting-adoption-european?utm>), and explanatory mutual-recognition discussions between Singapore, Australia, and New Zealand (Australian government Digital Identity, 2021).

including ECTA for e-signatures, POPIA for data protection, and a sophisticated payments and platform ecosystem. Its digitally delivered services exports are the largest in African in absolute terms (\$41.3 billion as of 2024). South Africa does not position digitalization as a cross-border trade agenda and lacks regional interoperability mechanisms for payments, data, or digital identity. South Africa represents a mature domestic digital economy without a regional digital-trade strategy.

Kenya has the strongest policy-level ambition toward digital trade on continent, explicitly framing cross-border e-commerce and regional integration as national objectives. However, its operational readiness remains limited. While Kenya's fintech ecosystem, especially M-Pesa enables some regional functionality, it lacks the institutional and regulatory systems required for formal digital trade, including cross-border data transfer rules, interoperable signatures, trust services, and digital ID recognition.

In this sense, Ethiopia is not late. Globally, only a handful of countries have advanced regional interoperability, and even these remain partial. What Ethiopia must ensure, however, is the strengthening of domestic digital infrastructure and trust architecture. Without minimally mature domestic system, including digital ID (functional authentication), trust services (national PKI, signature infrastructure), data protection law with functioning Data Protection Authority(DPA), payment interoperability, logistics digitization, and national addressing systems.

Table 4-6 Regional Benchmark Matrix for Digital-Trade Sequencing
(Rwanda, Kenya, Ghana, South Africa, and Ethiopia)

Country	Strategic Intent Toward Digital Trade*
Kenya	High. Kenya explicitly articulates the ambition to develop cross-border e-commerce and integrate into a continental digital market. Both the 2019 Digital Economy Blueprint and the 2023 National E-Commerce Strategy identify “regional digital trade” as a national priority. Declarative Leader. Kenya is the strongest in policy vision but significantly weaker in operational readiness. Strong intent, limited execution.
Ghana	Low. Ghana does not articulate a digital-trade agenda. Most reforms focus on trade facilitation, customs modernization, and revenue efficiency rather than digital services, data governance, or cross-border interoperability. Trade-Facilitation Modernizer. Strong on physical-trade digitalization, but no transition to the higher-order digital-trade layer (data, services, interoperability).
Rwanda	Medium–Low. Rwanda references “expanding digital services beyond national borders,” but does not frame digitalization explicitly as a regional trade agenda. Strategic documents focus on domestic digital-government integration, innovation ecosystems, and national service delivery. Institutional Integrator. Strong domestic DPI and governance, but weak regional extension. High execution but low cross-border strategic orientation.



Execution Reality (Systems, Institutions, Infrastructure)	Verified Evidence (Strategies, Laws, Reports)
Low–Medium. Kenya's fintech ecosystem (notably M-PESA) enables partial cross-border transactions within East Africa, and private-sector platforms operate regionally. However, Kenya lacks the regulatory and institutional foundations required for formalized digital trade: no cross-border data-transfer regime, no recognized trust-service system, incomplete e-signature interoperability, no digital-ID mutual recognition, and little evidence of digital-services export governance.	• National E-Commerce Strategy (2023): Defines e-commerce as “trade at a distance ... domestically and across borders.” • Digital Economy Blueprint (2019): Advocates for an “African Single Digital Market.” • WTO/UNCTAD data: Digitally delivered services exports remain modest; intra-African share extremely low (~3%).
Low. Ghana is a high performer in physical-trade modernization, including ICUMS, paperless ports, automated clearance, but digital trade components are missing: weak data-governance enforcement, no cross-border digital-ID use, no PKI mutual recognition, no cross-border payment interoperability, minimal digital-services export capacity. The ecosystem remains domestic.	• ICUMS & Paperless Port Reform: Strong customs digitalization. • ODI Digital Trade Implementation Report: Ghana “lacks a digital-trade strategy.” • WB Digital Economy Diagnostic (2021): Digital platforms remain domestic; digital-services exports are extremely low. • UNCTAD: Ghana's data-governance capacity is limited; enforcement weak.
High. Rwanda is Africa's most integrated digital public-infrastructure ecosystem: national ID (NIDA), RISA-led e-government backbone, integrated PKI, interoperable government services (IremboGov), and strong data-infrastructure governance. However, cross-border systems — digital-ID recognition, data-flow frameworks, trust-services interoperability — remain undeveloped. No structured digital-services export regime.	• ICT Sector Strategic Plan (2024–2029): Commits to growing digital content and services “beyond Rwanda.” • ITU Digital Regulation Case Study: Rwanda has one of Africa’s most mature gov-tech ecosystems. • WTO/UNCTAD: Rwanda classified as an “expanding but small-scale” digitally delivered services exporter.

Country	Strategic Intent Toward Digital Trade*
South Africa	Low. Despite a highly developed digital economy, South Africa does not frame digitalization as a cross-border trade agenda. National policies emphasize domestic modernization, privacy, cybersecurity, and consumer protection rather than AfCFTA-style digital-trade integration.
Ethiopia	Legal-Maturity Economy. Strongest legal and infrastructural foundation, but minimal cross-border framing. High execution, low regionalization. Low–Medium (nascent). Ethiopia's strategy documents focus on national digital-economy development, and do not explicitly address cross-border digital trade. AfCFTA alignment is acknowledged but not operationalized. No articulated vision for cross-border data governance, trust services, digital-services export, or regional interoperability. Foundational Stage. Ethiopia is in the earliest phase of digital-trade readiness, which is still consolidating domestic digital infrastructure, institutions, and regulations. A “domestic-first → interoperability later” strategy is most appropriate.

Execution Reality (Systems, Institutions, Infrastructure)	Verified Evidence (Strategies, Laws, Reports)
High. South Africa has Africa's most advanced legal-regulatory environment for digital markets: ECTA (advanced e-documents and e-signatures framework), POPIA (robust personal-data protection), Cybercrimes Act, strong financial-sector digital infrastructure, sophisticated trust-service providers, and a mature platform ecosystem. However, none of these systems are regionally interoperable, and there is no cross-border payment, data-transfer, or digital-ID recognition regime.	• ECTA (2002): Comprehensive e-signature and trust-service regime. • POPIA (2013): One of Africa's strongest data-protection frameworks. • UNCTAD Digital Economy Report (2024): SA = Africa's largest exporter of digitally delivered services (absolute terms) but minimal intra-Africa share.
Low. Ethiopia has foundational elements — Fayda digital ID rollout, early cloud strategy, cybersecurity expansion (INSA), draft data-protection law (2024), NBE's payment-sector reforms — but lacks operational systems for digital trade: no cross-border data rules, no PKI/trust-service recognition, no interoperable e-signature framework, limited digital-services export capacity, early-stage logistics digitization, and no national address system. Internet access and broadband quality remain LDC-level.	• WTO data in Digital Trade for Development Report: Ethiopia included in countries with growing digitally delivered services, but still small in absolute terms. • LDC connectivity data: Ethiopia's broadband capacity and internet penetration align with LDC averages (report pages 22–23). • Draft Personal Data Protection Proclamation (2024): Law passed but DPA not yet operational.

Note “Strategic intent toward digital trade” refers to the extent to which a country explicitly positions digital trade as a national priority in its official strategies, policies, and development plans. It measures how clearly and deliberately the government signals that cross-border digital commerce, digital services exports, data mobility, and regional digital-market integration are future directions for economic growth.

Table 4-7 Ethiopia's Structural Challenges and Comparative Lessons from Kenya, Rwanda, and South Africa in the Transition from E-Transactions to Digital Trade

Ethiopia's Structural Challenge	Rwanda: Institutional Consolidation Path	Ghana: Trade-Facilitation Digitalization Path
Balancing National and Regional Policy Logic	Built a centralized governance architecture through the Rwanda Information Society Authority (RISA), enabling whole-of-government digital coordination. Only after establishing internal coherence did Rwanda begin aligning with EAC interoperability standards (eIDAS-aligned trust services, digital ID verification, cross-border services under Smart Africa).	Ghana achieved one of Africa's strongest port and customs digitalization systems (GCNet → ICUMS) and modernized trade facilitation through the “Paperless Ports Reform.” However, digital transformation remains trade-centric, not economy-wide, and regional digital alignment (ECOWAS/AfCFTA) is not explicitly embedded in digital policy instruments.
Gap Between E-Transactions and Digital Trade	Rwanda expanded from transactional e-services (IremboGov) toward a full digital-product and services ecosystem (2024–2029 ICT Sector Strategic Plan), including local digital content, cross-border digital services, and trust architecture pilot programs.	Ghana's reforms strongly digitized customs processes, valuation, risk management, and introduced electronic payments in ports. Yet this digitalization remains transactional and logistics-focused; Ghana lacks frameworks for cross-border data flows, trust services, digital-product exports, or regional digital-ID interoperability.
Institutional Reluctance and Political Timing	Rwanda created a single coordination unit (RISA) with delegated authority and introduced sandbox-style pilots for digital identity, cross-border interoperability, and digital-services delivery before formal ratification — reducing political risk.	Ghana's progress reflects strong executive backing for trade facilitation, but institutional responsibility remains split (MoT, Ghana Revenue Authority, NCA, Bank of Ghana). There is no designated lead for digital trade governance, and policy timing is anchored in port reforms rather than a digital economy agenda.



Kenya : Market-Led Adaptation Path	South Africa : Legal Codification Path
Regional integration has been driven primarily by private-sector innovation, especially M-PESA, regional fintech corridors, and logistics platforms, while the government adopted regional norms only after the market matured. EAC and Smart Africa alignment evolved through industry demand rather than public-sector design.	South Africa embedded regional and international digital-trade principles directly into domestic law (e.g., POPIA (data), ECTA (e-signatures), Consumer Protection Act (cross-border clauses)). The approach is rule-first: codify norms domestically, then extend them to regional obligations (SADC/AfCFTA).
Kenya broadened beyond e-transactions via fintech and platform innovation, such as M-PESA APIs, iHub ecosystem, Ajira Digital jobs platform, creating functional digital-trade capabilities before major law reform. Practice led regulation.	South Africa codified both the form (e-signatures, documents, authentication, ECTA 2002) and the substance (privacy, data mobility , POPIA 2013) of digital trade. Legal completeness exists, but the trade framing (cross-border digital commerce) remains underdeveloped.
Kenya used regulatory sandboxes (Capital Markets Authority, communications regulator) and public–private partnerships to distribute political and operational risk, accelerating experimentation without waiting for comprehensive lawmaking.	South Africa separated regulatory responsibilities across agencies (DTIC for trade/ industry policy, ICASA for communications infrastructure, SARB for payments). This ensures continuity across political cycles but slows unified digital-trade coordination.

4.5. Strategic Entry Points for Ecosystem Integration

This chapter positions Fayda, Ethiopia's national digital identification system, as a foundational enabler of the country's digital economy. While the present advisory responds to MinT's request for legal and regulatory inputs on e-commerce and digital transaction frameworks, the analysis also identifies a broader strategic opportunity. From a systems perspective, a Fayda-based integration strategy could serve as an effective entry point for transitioning from a platform-based approach to a holistic e-commerce ecosystem. The objective is to enhance trust, transparency, and interoperability across digital transactions by linking Fayda's authentication capabilities with private-sector e-commerce and service platforms. Such integration is essential to ensure that Ethiopia's expanding digital ecosystem operates on a secure and accountable identity infrastructure.

Ethiopia's Fayda, digital ID system, operated by National ID Program (NIDP) provides a technical authentication foundation, including APIs that support biometric verification (face, finger, iris) and credential issuance (NIDP, 2025). This infrastructure offers a credible basis for linking to e-commerce platforms, although full operational integration with private-sector markets remains to be scaled.

More specifically, Fayda functions not merely as an identification database but as an API-based trust infrastructure capable of enabling biometric authentication and secure credential management at a national scale. Its architecture, which combines biometric data (fingerprint, face, iris) with a unique national identifier, already provides the technical and data foundation necessary for future interoperability with e-commerce, fintech, and digital government platforms. In policy terms, this capacity positions Fayda as a potential trust anchor for Ethiopia's broader digital ecosystem, which allows verified user identities, transactions traceability, and consumer protection mechanisms to be embedded into digital service delivery.

While Fayda is widely recognized both domestically and internationally as a cornerstone of Ethiopia's National Digital Economy Strategy, its current implementation strategy remains largely focused on awareness and public acceptance.²⁰

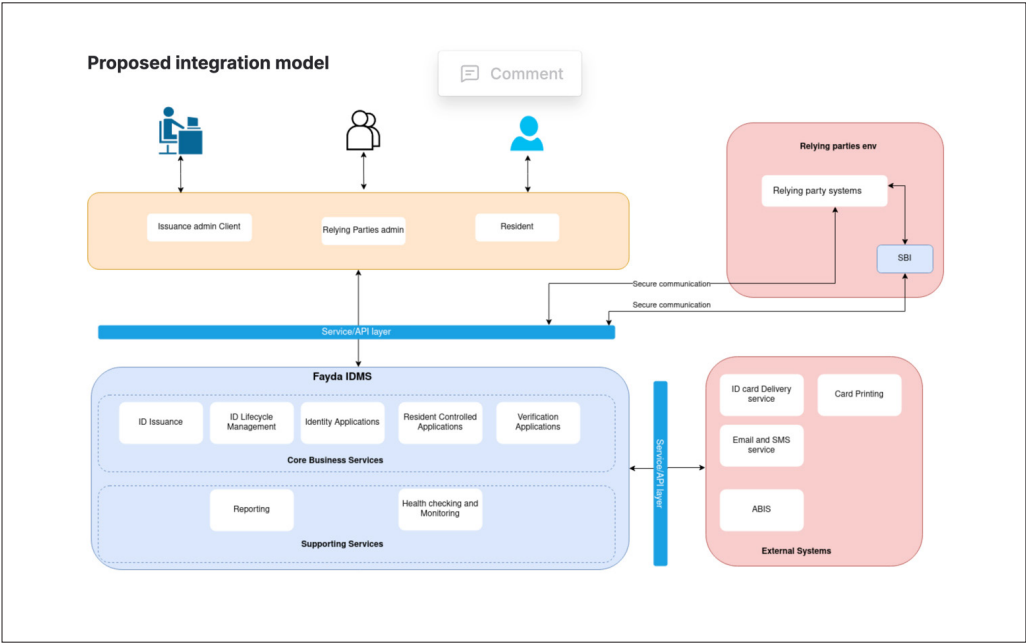
Comparable international frameworks, including World Bank's Digital ID Toolkit and the ITU's Digital Regulation Policy Roadmap, underscore that digital ID systems achieve impact only when paired with governance mechanisms that support multi-stakeholder

²⁰ While Fadya is currently receiving strategic advisory support from EY consulting, however, the scope of this consultancy primarily concerns communication and public awareness activities, including the design of campaign roadmaps, communication KPIs and content development plans. As such, the advisory work focusses on outreach and acceptance-building, rather than policy formulation, governance frameworks, or ecosystem integration strategies.

use-case activation. Accordingly, future advisory work could focus on formulating a policy activation strategy that operationalizes Fayda's integration into Ethiopia's e-commerce ecosystem through public-private partnerships and interoperable trust infrastructure.

As illustrated in [Figure 4-1], Fayda IDMS functions as the central identity management backbone, hosting core services such as ID assurance, lifecycle management, identity applications, resident-controlled applications, and verification modules. A service layer is positioned above this core to enable integration with external systems and facilitate interactions with relying parties.

Figure 4-1 Fayda Platform API Specification Proposed Integration Model



Source National Identification Program (NIDP) (n.d) Fayda Platform API Specification

Based on the integration model and the credential-printing workflow, Fayda currently provides a basic but functional digital-ID authentication service, centered on point-to-point verification between a relying party and the resident. The existing architecture allows service providers to request a Fayda Identification Number (FIN/FAN), receive consent through a one-time password (OTP), and then access a printable digital credential in PDF form. This is confirmed in the credential printing manual, which illustrates the step-by-step process: VPN setup, portal login, OTP verification, and finally PDF credential generation (see steps 1–6 in the Credential Printing Manual V.3).

[Figure 4-1] also shows that most interactions rely on secure communication layer rather than an interoperable trust-framework, and most relying-party across occurs through

custom portals rather than standardized APIs or federated authentication protocols.

For MinT, the figure reveals a structural constraint: the digital ID infrastructure exists, but it is not yet designed as a national trust platform that can anchor broader digital-economy functions. Because all external actors must integrate directly with Fayda through custom secure channels, the system does not yet support scalable integration with payments (NBE), e-commerce platforms, logistics operators, or government systems in a standardized way. In short, the [Figure 4-1] tells MinT that Fayda is technically centralized but institutionally isolated. This means MinT's role is not to modify Fayda's technical architecture, but to design the governance and interoperability framework that will allow this identity backbone to eventually support payments, e-signatures, digital documents, and—later—AfCFTA-level digital trade.

The Credential Manual V.3 reveal operational and procedural elements (OTP consent, credential printing, VPN/IP restrictions, data-seeding workflows, attribute-level KYC returns, and portal-based integration) that do not appear in the architectural figure, indicating that Fayda's real-world implementation is more constrained, manual, and institution-specific than the diagram alone suggests.

Fayda's current functionality, when based on FIN/FAN verification, OTP-based consent, demographic attribute return, and institution-specific integration, places Ethiopia firmly at the domestic e-KYC stage of digital-identity development. This is an important national milestone, but it also indicates that Ethiopia has not yet entered the trust-services layer required for full digital trade under the AfCFTA Digital Trade Protocol. At present, Fayda does not support electronic signatures, certificate authorities, timestamping services, trust lists, or any form of cross-border identity interoperability.

If the national ID ecosystem is still positioned at the domestic e-KYC level, then the broader e-commerce ecosystem is also necessarily in an early stage of maturity. Without interoperable authentication, recognized trust services, or cross-border data-governance mechanisms, Ethiopia's digital commerce remains structurally limited to domestic platform transactions. This means that e-commerce activity can expand in volume, but cannot yet transition into digital trade, which requires verifiable identities, secure digital documents, cross-border recognition, and integrated logistics and payments.

However, the system remains structurally constrained by its portal-centric, VPN-restricted, and institution-specific integration model, which limits scalability across the broader economy. More importantly, Fayda's present functionality covers only domestic identity verification. It does not include the trust-service components required under the AfCFTA Digital Trade Protocol—such as electronic signatures, certificate authorities, timestamping, electronic seals, or mutual recognition frameworks.

Table 4-8 **Fayda's Current Capabilities vs. AfCFTA Digital Trade Trust Requirements (Overview)**

Area	AfCFTA Requirement (Summary)	What Fayda Currently Provides (Based on Manuals)	Assessment
Electronic Identification & Authentication	Reliable digital identity, strong authentication, secure verification	FIN/FAN-based e-KYC; OTP consent; YES/NO verification; demographic attributes returned	Basic domestic authentication exists (early stage)
Trust Services (Art. 8–9)	Electronic signatures, electronic seals, timestamps, certificate services, registered delivery, trust-service governance	No such functions in manuals; PDF credential is not a trust service	Absent
Cross-border Trust & Mutual Recognition (Art. 19)	Interoperable digital ID; recognition of foreign trust services; standards for identity federation	No cross-border functionality or standards mentioned	Absent
Data Governance & Cross-border Data Flows (Art. 20–21)	DPA operation, lawful cross-border data transfer mechanisms, supervisory frameworks	No reference in Fayda manuals (handled by national law and other institutions)	Outside Fayda's scope; national-level gap remains
Integration with Payments, E-commerce, Logistics	Identity, KYC, trust infrastructure supporting payments, online commerce, logistics and customs	Currently limited to e-KYC for financial institutions and data-seeding for NBE onboarding	Narrow financial-sector integration only

However, this topic was not part of the initial request for this Year-1 advisory and has not yet been the subject of inter-agency consensus. Because the integration of national ID into digital trade frameworks requires coordination with NIDP, INSA, the Ministry of Justice, NBE, and other actors, a full assessment would exceed the scope of the current advisory phase.

Therefore, digital ID is identified here as a forward-looking issue to be examined systematically in Year 2, when institutional readiness and implementation pathways can be analysed in depth.

4.6. Concluding Considerations

While the expansion of digital trade may appear premature for Ethiopia at this stage, the present moment is not one of absence, but of foundational construction. Ethiopia is building the minimum institutional and infrastructural layers on which any credible digital-trade system must eventually rest. The immediate policy priority is therefore not rapid regional integration, but the deliberate sequencing of domestic reforms: consolidating digital infrastructure, strengthening legal instruments, and clarifying institutional mandates. These elements will form the preconditions for Ethiopia's future participation in regional interoperability mechanisms under the AfCFTA framework.

This report has also shown that Ethiopia currently sits at what may be described as the “pre-interoperability” phase, which is a stage observed across all countries before they move toward cross-border digital trade readiness. This is neither a weakness nor a delay: none of the benchmark African countries examined, including Rwanda, Kenya, Ghana, or South Africa, have fully operationalized the digital-trade architecture envisioned under the AfCFTA Digital Trade Protocol.

This report has also shown that Ethiopia currently sits at what may be described as the “pre-interoperability” phase—a stage observed across all countries before they move toward cross-border digital trade readiness. This is neither a weakness nor a delay: none of the benchmark African countries, including Rwanda, Kenya, Ghana, or South Africa examined, have fully operationalized the digital-trade architecture envisioned under the AfCFTA Digital Trade Protocol. Each remains at a partial stage of ecosystem development, building domestic systems first and deferring cross-border interoperability until foundational mechanisms are secure. Ethiopia's present trajectory therefore mirrors the natural progression observed across the continent.

Because digital trade governance spans multiple sovereign regulatory domains, including payments, identity, cybersecurity, data protection, logistics, customs, competition policy, and trust services; it requires multi-year technical scoping, legal drafting, and inter-agency negotiation that exceed what any strategy-development process can contain. For this reason, a report of this scope cannot credibly deliver a full operational governance architecture, and even an entire second-year advisory phase cannot realistically cover the entire cross-border digital-trade system. What is feasible, and what this report aims to provide, is a structured analytical foundation: clarifying the governance logic of the AfCFTA Digital Trade Protocol, identifying Ethiopia's institutional and infrastructural gaps, and outlining the sequencing principles that will guide Ethiopia's transition from domestic digital-economy development toward future regional interoperability.

In this sense, the core purpose of the report has been threefold:

- 1) to establish conceptual clarity regarding what AfCFTA digital-trade alignment truly requires;
- 2) to diagnose Ethiopia's current structural, governance, and institutional constraints through a detailed reading of its Digital Economy Strategy and related frameworks; and
- 3) to situate Ethiopia's trajectory within a comparative African context by examining how Rwanda, Kenya, Ghana, and South Africa are addressing similar challenges.

These analytical components together provide a grounded basis for Ethiopia's long-term digital-trade strategy. They do not prescribe immediate solutions, nor do they claim to resolve cross-border governance questions within the current advisory year. Instead, they define the nature of the challenge, clarify institutional realities, and establish the foundation on which future, more detailed implementation work, including digital ID integration and governance-architecture design can be responsibly undertaken in the next advisory phase.

Taken together, the legal and standards outputs presented in this report constitute a foundational framework for Ethiopia's evolving e-commerce ecosystem. While the primary focus of the first year has been on establishing coherent regulatory and technical underpinnings, the strategic considerations discussed in this chapter underscore the importance of phased implementation, institutional coordination, and practical learning over time. In this sense, the value of the first-year consultation lies not only in the individual outputs themselves, but in their potential to support a gradual transition from design to application, enabling Ethiopia to translate regulatory frameworks into operational practice in a manner aligned with its institutional capacity and development trajectory.

References

CONSULTATION ON ETHIOPIA'S E-COMMERCE LEGAL AND STANDARDS FRAMEWORKS

- Blind, K. (2013). *The Impact of Standardization and Standards on Innovation*. Nesta Working Paper 13/15, November 2013. https://media.nesta.org.uk/documents/the_impact_of_standardization_and_standards_on_innovation.pdf
- Cole, Mark D., Christina Etteldorf, and Carsten Ullrich. (2020). *Cross Border Dissemination of Online Content: Current and Possible Future Regulation of the Online Environment with a Focus on the EU E-Commerce Directive*. Nomos.
- Communications Authority of Kenya. (2023). *National E-Commerce Strategy (2023)*. Nairobi: CA Kenya. Retrieved from <https://www.ca.go.ke/sites/default/files/CA/E-Commerce%20Strategy/National%20E-Commerce%20Strategy%20%202023.pdf>
- DiMatteo, Larry A., Michel Cannarsa, and Cristina Poncibò (eds.). (2019). *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*. Cambridge University Press.
- Diplomacy.edu / Smart Africa. (2023). *Digital Economy in Africa: National Policy and Regulatory Frameworks*. Retrieved from <https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-economy-africa-national-policy-regulatory-frameworks/>
- Government of Korea. (2016). *Framework Act on Electronic Documents and Transactions* (Revision 2016, not current). Retrieved from <https://www.law.go.kr/LSW/lsInfoP.do?lsISeq=179518&chrClsCd=010203&urlMode=engLsInfoR&viewCls=engLsInfoR#EJ18:0>
- Government of South Africa. (2002). *Electronic Communications and Transactions Act 25 of 2002*. Pretoria: Government Gazette. Retrieved from <https://www.gov.za/documents/electronic-communications-and-transactions-act>
- Government of South Africa. (2013). *Protection of Personal Information Act 4 of 2013*. Pretoria: Government Gazette. Retrieved from <https://www.gov.za/documents/protection-personal-information-act>
- Government of South Africa. (2020). *Cybercrimes Act 19 of 2020*. Pretoria: Government Gazette. Retrieved from <https://www.gov.za/documents/cybercrimes-act-19-2020-english-2021-12-01>
- International Organization for Standardization (ISO). (n.d.). *Standards*. Retrieved from <https://www.iso.org/standards.html>

- International Telecommunication Union (ITU). (2023). *Collaborative Regulation Case Study: Rwanda*. Geneva: ITU Telecommunication Development Sector. Retrieved from https://digitalregulation.org/wp-content/uploads/Collaborative-Regulation_Case-Study-Rwanda_Final_E-1.pdf
- ISO/TC 321. (n.d.). *ISO/TC 321 Transaction Assurance in E-Commerce*. Retrieved from <https://www.iso.org/committee/7145156.html>
- Judicial Research and Training Institute. (2011). *Study on Electronic Transactions Law*. Judicial Research and Training Institute. (in Korean)
- Ministry of Finance and Economic Planning (MINICOFIN). (2024). *ICT Sector Strategic Plan (2024–2029)*. Kigali: Government of Rwanda. Retrieved from <https://www.minecofin.gov.rw/>
- Ministry of Information, Communications and Technology (MoICT). (2019). *Digital Economy Blueprint: Powering Kenya's Transformation*. Nairobi: Government of Kenya. Retrieved from <https://www.ict.go.ke/digital-economy-blueprint/>
- Ministry of Trade & Regional Integration, Federal Democratic Republic of Ethiopia. (n.d.). *National E-Commerce Strategy (Draft version)*.
- National Identification Program (NIDP). (n.d.). *Fayda Platform API Specification*. Atlassian Confluence. Retrieved October 21, 2025, from <https://nidp.atlassian.net/wiki/spaces/FAPIQ/pages/633733136/Fayda%2BPlatform%2BAPI%2BSpecification>
- Sohn, Jinhwa, and Jaebeom Kim. (2022). *Law of Electronic Commerce*. Sinjosa. (in Korean)
- Todd, Paul. (2005). *E-Commerce Law*. Cavendish Publishing.
- U.S. Department of Commerce. (2024). *Kenya – E-Commerce Country Commercial Guide*. Washington, DC: Trade.gov. Retrieved from <https://www.trade.gov/country-commercial-guides/kenya-ecommerce>
- United Nations Conference on Trade and Development (UNCTAD). (2025). *E-Commerce and Digital Economy Programme: Year in Review 2024*.
- United Nations Conference on Trade and Development (UNCTAD). (2025). *Fast Tracking Implementation of Reforms Enabling E-Commerce and Digital Trade*.
- United Nations Economic Commission for Europe (UNECE). (n.d.). *Trade Facilitation and E-business (UN/CEFACT)*. Retrieved from <https://unece.org/trade/uncefact>
- Wang, Faye Fangfei. (2010). *Law of Electronic Commercial Transactions*. Routledge.
- World Trade Organization (WTO). (n.d.). *Technical Barriers to Trade*. Retrieved from https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm

Annex

CONSULTATION ON ETHIOPIA'S E-COMMERCE LEGAL AND STANDARDS FRAMEWORKS

1. Sample Korean Laws and Regulations related to e-Trust Mark Certification

1. FRAMEWORK ACT ON ELECTRONIC DOCUMENTS AND TRANSACTIONS (2008–2016)²¹

Article 18 (Certification of Electric Transaction Business Entities) (1) The Minister of Science, ICT and Future Planning may certify an exemplary electric transaction business entity in order to promote electronic transactions and protect electronic transaction users. <Amended by Act No. 11690, Mar. 23, 2013>

(2) The Minister of Science, ICT and Future Planning may collect fees from a person who files for certification under paragraph (1). <Amended by Act No. 11690, Mar. 23, 2013>

(3) Standards and procedures for certification under paragraph (1) and fees collected under paragraph (2) and other necessary matters shall be prescribed by Presidential Decree.

[This Article Wholly Amended by Act No. 11461, Jun. 1, 2012]

Article 18-2 (Certification Marks) (1) Any electronic transaction business entity that has obtained certification (hereinafter referred to as “exemplary electronic transaction business entity”) under Article 18 (1) may use a certification mark of an excellent electronic transaction business entity (including a mark by any electronic means, such as the Internet; hereinafter the same shall apply), as prescribed by Presidential Decree.

(2) No person, other than an exemplary electronic transaction business entity, shall use a certification mark referred to in paragraph (1) or a similar mark similar thereto, or publicize him/her as such.

²¹ <https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=179518&lsId=002000&chrClsCd=010202&urlMode=lsInfoP&viewCls=lsInfoP&efYd=20160204&vSct=&ancYnChk=undefined#0000>

[This Article Newly Inserted Amended by Act No. 11461, Jun. 1, 2012]

Article 18-3 (Revocation of Certification) Where an electronic transaction business entity falls under any of the following cases, the Minister of Science, ICT and Future Planning may revoke certification granted under Article 18 (1): Provided, That where it falls under subparagraph 1, he/she shall revoke its certification: <Amended by Act No. 11690, Mar. 23, 2013>

1. Where it has obtained certification by fraudulent or other unlawful means;
2. Where it has violated matters to be generally observed by an electronic transaction business entity under Article 17;
3. Where it has failed to meet standards for certification under Article 18 (3).

[This Article Newly Inserted by Act No. 11461, Jun. 1, 2012]

Article 18-4 (Registration of Certified Electronic Addresses) (1) Any person who intends to send or receive electronic documents using his/her certified electronic address shall register his/her certified electronic address with the exclusively responsible agency under Article 22 (1).

(2) Upon receipt of an application for registration under paragraph (1), the exclusively responsible agency under Article 22 (1) shall confirm whether a certified electronic address applied for registration conforms to international standards, etc., and enter and store the details thereof in an information processing system.

(3) The exclusively responsible agency under Article 22 (1) may collect fees from persons who apply for registration pursuant to paragraph (1).

(4) Matters necessary for registration and storage of certified electronic addresses and registration fees under paragraphs (1) through (3) shall be prescribed by Ordinance of the Ministry of Science, ICT and Future Planning. <Amended by Act No. 11690, Mar. 23, 2013>

[This Article Newly Inserted by Act No. 11461, Jun. 1, 2012]

Article 18-5 (Generation and Issuance of Distribution Certificates, etc.) (1) Where an electronic document is sent, received or read through a certified electronic address, the exclusively responsible agency under Article 22 (1) shall generate and store information including the following matters (hereinafter referred to as “distribution information”):

1. Time the electronic document is sent and received;
2. The sender and the addressee of the electronic document;
3. Other matters prescribed by Presidential Decree concerning transmission and receipt of electronic documents.

(2) An originator and a sender may be issued a distribution certificate from

the exclusively responsible agency under Article 22 (1), which stores distribution information.

(3) Where the exclusively responsible agency under Article 22 (1) has issued a distribution certificate according to the method and procedure prescribed by Presidential Decree, such distribution certificate shall be presumed true and correct.

(4) Matters necessary for the generation, storage and issuance of distribution certificates under paragraphs (1) and (2) shall be prescribed by Presidential Decree.

[This Article Newly Inserted by Act No. 11461, Jun. 1, 2012]

Article 18-6 (Prohibition of Collection, etc. of Certified Electronic Addresses through Automated Programs, etc.) (1) No one shall collect certified electronic addresses through an automated program or technical mechanism that collects certified electronic addresses.

(2) No person shall sell or provide any collected certified electronic address in violation of paragraph (1).

[This Article Newly Inserted by Act No. 11461, Jun. 1, 2012]

Article 18-7 (Prohibition of Sending Advertisements) No one shall send any advertisement to the certified electronic address of any addressee for the purpose of profit-making or public relations.

[This Article Newly Inserted by Act No. 11461, Jun. 1, 2012]

Article 22 (Agency Exclusively Responsible for Promoting Use of Electronic Documents and Conduct of Electronic Transactions) (1) The Ministry of Science, Information and Communications Technology (ICT) and Future Planning may designate an exclusively responsible agency to implement the following projects in an efficient and systematic manner for facilitating the use of electronic documents as well as the conduct of electronic transactions: <Amended by Act No. 13347, Jun. 22, 2015>

1. Support for certification of facilities or equipment creating digitized documents under Article 23 (3);
2. Research and development and dissemination projects of standards related to electronic documents and electronic transactions under Article 24, and activities related to the international standardization of such standards;
3. Support for technical development under Article 25;

4. Support for fact-finding surveys of statistics on electronic documents and electronic transactions under Article 28;
5. Support for duties of designating certified electronic document centers under Article 31-2;
6. Support for reporting of working rules, such as the storage of electronic documents, under Article 31-8;
7. Support for technologies on measures for protecting electronic documents by certified electronic document centers under Article 31-9 (3);
8. Acquiring stored documents, etc. under Article 31-15 (3);
9. Support for duties of designating certified electronic documents intermediaries under Article 31-18;
10. Operation of the Mediation Committee of Disputes on Electronic Documents and Transactions under Article 32.

(2) The exclusively responsible agency may collect fees from persons who apply for certification under paragraph (1) 1, as prescribed by Ordinance of the Ministry of Science, ICT and Future Planning. <Amended by Act No. 11690, Mar. 23, 2013>

(3) The Government may fully or partially subsidize expenses incurred by the exclusively responsible agency in performing projects to facilitate the conduct of electronic transactions and the use of electronic documents within budgetary limits or within the Information and Communication Technology Promotion Fund established under Article 41 of the Information and Communications Technology Industry Promotion Act.

[This Article Wholly Amended by Act No. 11461, Jun. 1, 2012]

Policy Material 25-17-02

CONSULTATION ON
ETHIOPIA'S E-COMMERCE LEGAL
AND STANDARDS FRAMEWORKS

발행인 | 이상규

발행처 | 정보통신정책연구원

충청북도 진천군 덕산읍 정통로 18

Tel. 043-531-4416 Fax. 043-531-4419

디자인 | 시드그래피 seedgraphy@naver.com

KISDI

18, Jeongtong-ro, Deoksan-myeon, Jincheon-gun,
Chungcheongbuk-do, 28982, Republic of Korea
Tel. +82-43-531-4416 Fax. +82-43-531-4419
www.kisdi.re.kr