RESEARCH PAPER

Securing Ethiopia's Digital Government Ecosystem through a Context-Aware Cybersecurity Framework for the Mesob Ecosystem under the Digital Ethiopia 2030 Strategy

Dr. Tilahun Ejigu Belay[1], Dr. Shalu Gupta[2]
[1]Cybersecurity Researcher, Dept. of Computer Applications, Guru Kashi University, Talwandi Sabo, Punjab, India
[2]Associate Professor, Dept. of Computer Applications, Guru Kashi University, Talwandi Sabo, Punjab, India

Received: 25th May, 2026; **Revised:** 6th June, 2026; **Accepted:** 8th June, 2026; **Available Online:** 17th June, 2026

ABSTRACT
Ethiopia is making rapid strides towards digital transformation under the Digital Ethiopia 2030 (DE2030) Strategy by expanding digital government services, interoperable platforms and applications, and cloud computing, digital identity systems, and integrated public service infrastructures. The Mesob Digital Collaboration Ecosystem has become a strategic platform that allows for the secure collaboration, sharing of information and coordinated provisioning of services between government institutions and stakeholders. At the same time as growing connectivity among digital systems has opened doors for new opportunities, it has also opened the door for cyber threats like data breaches, ransomware attacks, unauthorized access, API vulnerabilities and attacks against critical national infrastructure.
This paper proposes a Context-Aware Cybersecurity Framework that would enhance the security, resiliency and interoperability of Ethiopia's digital government ecosystem. The framework encompasses adaptive security features such as Zero Trust Architecture, Identity and Access Management (IAM), secure interoperability security, continuous monitoring, threat intelligence, and risk-based access control, all designed to tackle the evolving nature of cybersecurity in today's interconnected digital landscape.
The framework proposed has the potential to contribute to a secure and stable digital governance, the protection of critical digital infrastructures, and the sustainable digital transformation process, as outlined in the DE2030 strategy. It also offers a localized cybersecurity model which is aligned to Ethiopia's technological, institutional and digital governance context to increase cyber resilience and build trust in digital public services.
Keywords: Cybersecurity Framework, Context-Aware Security, Mesob Digital Ecosystem, Digital Ethiopia 2030, Zero Trust Architecture, Digital Government, Secure Interoperability, Identity and Access Management (IAM), Cyber Resilience, Digital Governance, Cloud Security, API Security, Digital Identity, Continuous Monitoring, Ethiopia.
How to cite this article: Belay TE, Gupta S. Securing Ethiopia's Digital Government Ecosystem through a Context-Aware Cybersecurity Framework for the Mesob Ecosystem under the Digital Ethiopia 2030 Strategy. Int J Drug Deliv Technol. 2026;16(61s): 330-372. DOI: 10.25258/ijddt.16.61s.40
Source of support: Nil.
Conflict of interest: None.

1. Introduction

Ethiopia is undergoing digital transformation with the launch of the national Digital Ethiopia 2030 strategy which aims to modernize public services, increase digital infrastructure, boost the digital economy and digital governance in public and private sectors. It aims to maximize the use of information and communication technologies (ICTs), cloud computing, mobile platforms, interoperable systems, and digital innovation for enhancing the delivery of services, institutional efficiency, economic development and citizen engagement. The importance of safe, scalable, and collaborative digital environments has moved to the top of the government and organizational agenda as digital technologies grow more prevalent in government and organizational operations.

The Mesob Digital Collaboration Ecosystem is a culturally driven approach to secure and interoperable digital collaboration as part of this transformation agenda. The word “Mesob” (which is traditionally understood in Ethiopian culture as a sign of unity, sharing, cooperation and collective engagement) is a concept for connected digital governance and institutional cooperation. In digital, the Mesob ecosystem is an interconnected environment in which government institutions, private organizations, businesses and the citizens can communicate and exchange information, connect workflows, offer digital services and enable coordinated decision

making, all within secure platforms and digital infrastructures.

While digital transformation creates opportunities, digital interconnectivity comes with great challenges in the field of cybersecurity. Cloud platforms, APIs, mobile apps, co-shared infrastructure, and databases are now ubiquitous, increasing the attack surface of digital systems and leaving behind dangerous cyber threats for organizations. Unauthorized access, data breaches, ransomware attacks, service disruption, insider threats, API exploits, critical national infrastructure attacks, cyber espionage, identity theft. These risks might undermine the trust, availability, integrity and confidentiality of shared digital spaces. Current cyber security frameworks and security models are generally developed for wide global contexts and may not be able to cater to Ethiopia's technological, organizational, cultural, regulatory, and socio-economic contexts. Ethiopia's digital transformation context demands a localized and context-specific cybersecurity strategy due to factors like limited cybersecurity maturity, inconsistent governance, evolving digital policies, infrastructure limitations, and varying institutional capabilities.

This study recommends a Context-Aware Cybersecurity Framework for the security of Ethiopia's Mesob Digital Collaboration Ecosystem under the Digital Ethiopia 2030 Strategy as a solution to these challenges. Proposed framework features contextual intelligence, adaptive security controls, identity and access management, continuous monitoring, risk-based decision-making, governance mechanisms and threat intelligence capabilities to enhance cybersecurity resilience to interconnected digital platforms. Additionally, it provides the ability to adapt dynamically to evolving operational environments, user habits, vulnerabilities in systems, and new cyber threats, while ensuring secure interoperability and trusted digital collaboration between institutions.

The research will play a crucial role in ensuring digital governance, institutional trust, interoperability, safeguarding critical digital assets, secure information exchange, and the sustainability of Ethiopia's digital transformation efforts. Moreover, the study aims to propose a localized cyber security model that matches the technological security needs and Ethiopia's cultural values, governance concerns and national digital development goals were discussed and aware on the following main point.

- Elaboration of a context-aware cybersecurity framework specific to the context of Ethiopia's Digital Transformation.
- Improvements to secure interoperability and trusted digital collaboration in the Mesob Digital Collaboration Ecosystem.
- Implementing cutting-edge cybersecurity technologies and solutions like Zero Trust, IAM, continuous monitoring and threat intelligence.
- Enhancements of national cyber-resilience, digital governance and critical digital infrastructure protection within the framework of Digital Ethiopia 2030 Strategy.

2.1 Background of the Study

The Mesob Digital Collaboration Ecosystem has become an integral part of the wider digital transformation effort in Ethiopia, encapsulated within the Digital Ethiopia 2030 (DE2030) Strategy. It has a long history, closely linked with the process of modernisation of public service delivery, the efficiency of public administration and the reduction of institutional fragmentation among public institutions. The public service system was traditionally paper-intensive, manually operated, and lacked inter-agency collaboration, with each ministry and public agency using its own information system. A lack of integrated digital infrastructure led to inefficiencies in operations, duplication of data, long service delivery cycles, insufficient inter-agency coordination, and limited access to citizens for fast and efficient public services.

First steps to address these challenges were taken at national level in the digital Ethiopia 2025 strategy, particularly in terms of expanding ICT infrastructure, universal connectivity and the provision of elementary services in e-government. This approach laid the groundwork for technological innovations in digital transformation, yet it also identified critical institutional coordination, data sharing, and interoperability challenges. Government institutions remained isolated in a digital world and many information systems lacked common communication protocols for an integrated service delivery. The overall effectiveness of early DT initiatives continues to be limited in scope.

To address these challenges, Ethiopia has developed a more advanced, integrated and ecosystem focused national digital transformation framework called the Digital Ethiopia 2030 Strategy. DE2030 focuses on interoperable, digital ecosystems, data-driven governance, institutional integration and coordinated digital service delivery across various sectors, rather than on the digitization of individual services, as was required by previous approaches. In this strategic transition, the concept of the Mesob Digital Collaboration Ecosystem to bring together institutions, digital interoperability and governance in a unified framework was introduced.

"Mesob" comes from the traditional woven basket that is used for communal eating in Ethiopia which represents unity, inclusiveness, cooperation and collective participation. The Mesob concept was further translated into the digital governance sphere as an interconnected digital ecosystem where government organizations, institutions and stakeholders share infrastructure, services, workflow and data in a secure manner and based on a common digital framework. The Mesob ecosystem was thus conceived not as a single software product, but as an interoperability and collaboration system across multiple institutions that will enable smooth communication and coordinated service delivery between public institutions.

The initial phase of the Mesob ecosystem implementation started with the development of one-stop service delivery centers which aim to integrate multiple government services into a single operating environment. It aimed to increase citizen access to public services, minimize administrative complexity and institutional fragmentation. Over time, these physical-based service integration efforts grew into digital platforms that integrated services like national ID, immigration management, taxation, investment licensing, civil registration, and public administration. However, with the growing adoption of digital, it was clear that aggregation of services would not be enough to enable efficient digital governance and real-time institutional collaboration.

The Mesob Digital Collaboration Ecosystem gradually became an all-encompassing framework of interoperability and integration, including new digital governance technologies. This change brought in the digital identity management systems, API-based data exchange mechanisms, centralized authentication services, and interoperable communication infrastructures, which facilitated secure and efficient data exchange between institutions. Over time, the ecosystem gradually grew to include the national digital governance platforms as well as federal ministries, regional governments, financial institutions, telecommunication companies, etc.

The Mesob ecosystem is a key component in the Digital Ethiopia 2030 agenda, which aims to deliver citizen-centered governance, minimizing administrative fragmentation, increase institutional interoperability and promote development of the digital economy. The ecosystem allows citizens to access various services from the government from a single gateway via digital means and institutions to exchange information and coordinate activities in real time. This holistic strategy leads to more efficient services, lower service costs, increased transparency and accountability, and more effective public services.

The Mesob Digital Collaboration Ecosystem has become a key component of Ethiopia's digital transformation strategy today. It marks a shift from disjointed and separate digital projects to a coherent, national digital framework, with an increased focus on interoperability, multi-agency management, secure information sharing and data-enabled public service provision. The history of its development illustrates the overall progression of Ethiopia's digitalization efforts, which aim to create a unified digital Ethiopia with government actors as integrated parts of a secure and collaborative digital environment.

Digital Ethiopia 2030 and Meson Digital Collaboration Ecosystem was created in the Background

- The Digital Ethiopia 2030 (DE2030) Strategy will transform Ethiopia's public services, deepen the digital governance, and build the interoperability of digital systems and institutional integration.
- Inspired by the cultural notion of collective participation, inclusiveness, and cooperation in Ethiopia, the Mesob Digital Collaboration Ecosystem was introduced as a unified digital governance system.
- The previous digital government systems in Ethiopia were not integrated, connected, and manual/paper-based, which led to inefficiency, duplication of services, and inadequate institutional coordination.
- The development of the Mesob ecosystem brought in more sophisticated technologies like digital identity systems, API-based interoperability, centralised authentication services, and secure communication infrastructure for effective and secure digital governance.

The figure below demonstrates how the Mesob Integrated System serves as a centralized digital collaboration platform that integrates government institutions, private sector organizations, and citizens through secure and interoperable digital technologies. Digital Security provides the foundational protection mechanisms necessary for secure data exchange, cybersecurity governance, digital identity protection, and national cyber resilience. Digital Ethiopia 2030 acts as the national strategic vision guiding digital modernization, innovation, digital inclusion, and technology-driven economic growth. Citizen-centered services focus on delivering accessible, efficient, transparent, and integrated digital services such as e-government, digital banking, e-health, and e-education systems. The figure also highlights the critical role of multi-sector stakeholders, including government institutions, private sector organizations, research

institutions, development partners, and digital communities, in accelerating Ethiopia's secure, inclusive, and sustainable digital transformation journey.

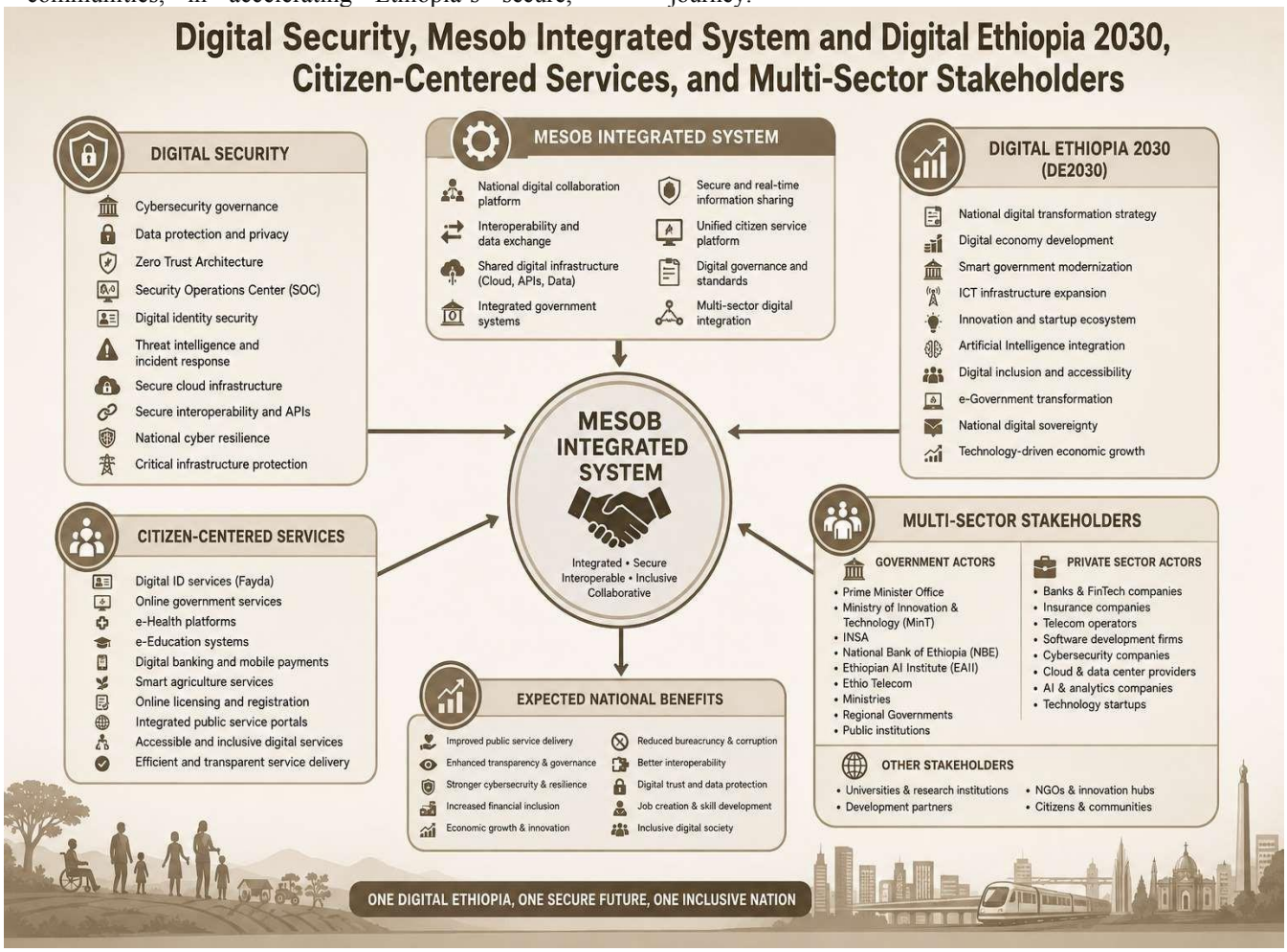

Figure 1, illustrates the relationship between Digital Security, the Mesob Integrated System, Digital Ethiopia 2030 (DE2030), Citizen-Centered Services, and Multi-Sector Stakeholders

Digital Security, Meson Integrated System, Digital Ethiopia 2030, Citizen-Centered Services, and Multi-Sector Stakeholders		
Component	**Key Areas**	**Description**
1. Digital Security	Cybersecurity governance	Establishes national cybersecurity policies, standards, and governance mechanisms.
	Data protection and privacy	Protects citizen and institutional data from unauthorized access and misuse.
	Zero Trust Architecture	Ensures continuous verification of users, devices, and systems.
	Security Operations Center (SOC)	Provides real-time monitoring, threat detection, and incident response.
	Digital identity security	Secures digital identity systems such as Fayda Digital ID.
	Threat intelligence and incident response	Identifies cyber threats and supports rapid response mechanisms.
	Secure cloud infrastructure	Protects cloud platforms, national data centers, and digital services.

	National cyber resilience	Strengthens Ethiopia's ability to resist and recover from cyberattacks.
	Secure interoperability and APIs	Enables secure communication and data exchange among systems.
	Critical infrastructure protection	Protects essential national digital and communication infrastructure.
2. Mesob Integrated System	**National digital collaboration ecosystem**	**Connects government, private sector, and citizens through digital platforms.**
	Interoperability platform	Enables integrated communication among institutions.
	Shared digital infrastructure	Supports shared cloud, network, and digital platforms.
	Integrated government systems	Connects ministries and public institutions digitally.
	Secure data exchange	Allows secure sharing of national information and services.
	Digital governance framework	Supports policy implementation and digital coordination.
	Unified citizen service platform	Provides integrated digital services for citizens.
	Multi-sector digital integration	Connects finance, telecom, health, education, and other sectors.
	Cloud and API integration	Enables scalable digital services and interoperability.
	Real-time institutional collaboration	Improves coordination among institutions and stakeholders.
3. Digital Ethiopia 2030 (DE2030)	**National digital transformation strategy**	**Ethiopia's roadmap for digital modernization and innovation.**
	Digital economy development	Promotes technology-driven economic growth.
	Smart government modernization	Modernizes public services through digital technologies.
	ICT infrastructure expansion	Expands broadband, telecom, and digital infrastructure.
	Innovation and startup ecosystem	Encourages innovation, entrepreneurship, and digital startups.
	Artificial Intelligence integration	Supports AI adoption in government and business sectors.
	Digital inclusion and accessibility	Expands digital access to all citizens and communities.
	e-Government transformation	Enables online and integrated government services.
	National digital sovereignty	Protects Ethiopia's national digital interests and systems.
	Technology-driven economic growth	Supports sustainable digital economic development.
4. Citizen-Centered Services	**Digital ID services (Fayda)**	**Provides trusted digital identity and authentication services.**
	Online government services	Enables digital access to government services and information.
	e-Health platforms	Supports digital healthcare systems and patient services.
	e-Education systems	Expands online learning and digital education platforms.
	Digital banking and mobile payments	Enhances financial inclusion and digital transactions.
	Smart agriculture services	Supports farmers through digital agricultural solutions.

	Online licensing and registration	Simplifies public licensing and registration processes.
	Integrated public service portals	Provides centralized citizen service access.
	Accessible and inclusive digital services	Ensures equal digital access for all citizens.
	Efficient and transparent service delivery	Improves public trust, speed, and accountability.
5. Multi-Sector Stakeholders	**Government Actors**	**Prime Minister Office, MInT, INSA, NBE, Ethio Telecom, EAII, Ministries, and Regional Governments.**
	Private Sector Actors	Banks, FinTech companies, telecom providers, software firms, cybersecurity companies, cloud providers, AI companies, and startups.
	Other Stakeholders	Universities, research institutions, development partners, NGOs, innovation hubs, citizens, and digital communities.
6. Expected National Benefits	**Secure digital transformation**	**Builds a secure and resilient national digital ecosystem.**
	Improved public service delivery	Enhances accessibility and efficiency of government services.
	Enhanced cybersecurity maturity	Strengthens national cyber defense and resilience.
	Increased financial inclusion	Expands digital financial services to citizens.
	Economic growth and innovation	Encourages investment, innovation, and entrepreneurship.
	Improved transparency and governance	Supports accountability and good governance.
	Digital trust and resilience	Builds confidence in digital systems and platforms.
	Reduced bureaucracy and corruption	Simplifies processes and improves transparency.
	Better interoperability	Improves collaboration among institutions and sectors.
	Inclusive digital society	Promotes equal digital participation and accessibility.

2.1.1 Digital Ethiopia 2030 as Strategic Foundation and Operational Foundation of Mesob

Digital Ethiopia 2030 (DE2030) is the national strategic foundation for the digital transformation agenda and the Mesob Digital Collaboration Ecosystem is the operational and integration foundation that supports the realization of the vision in the interconnected government institutions and digital platforms of the country. These combine to create a cohesive national digital governance ecosystem that seeks to digitalize public services, deepen inter-institutional cooperation, enhance cybersecurity resilience, and embed a durable socio-economic development strategy using cutting-edge digital technologies.

Digital Ethiopia 2030 is the overall vision and policy guidance for the nation's journey towards becoming a digitally empowered economy and a knowledge-based economy. Digital governance, digital infrastructure development, cybersecurity enhancement, artificial intelligence and data governance, citizen-centered digital services and modernization of the digital economy are among the strategy's main pillars. Together these pillars serve as a blueprint for the nation's journey from a silo, manual and paper-centered governance system into an integrated, interoperable and technology-enabled system.

Digital government is one of the key strategic thrusts of Digital Ethiopia 2030. It includes modernization of government operations as e-government, interoperable digital platforms and integrated service delivery. The goal is to transform public services using digital technology in order to enhance their efficiency, transparency, accountability and accessibility. The Mesob Digital Collaboration Ecosystem serves as the operational integration platform to link ministries, agencies, regional governments and public institutions into a synchronized digital governance ecosystem within this strategic direction.

Development of digital infrastructure is also a crucial aspect of the DE2030 strategy. The success of Ethiopia's digital transformation relies on the

availability of the necessary infrastructure to support a digital economy, which consists of cloud computing systems, internet of things, broadband networks, government data centers, digital identity systems, mobile communication platforms, and secure national connectivity infrastructures. These common infrastructures enable real-time communications, interoperability between institutions, data sharing and multi government digital services within the Mesob ecosystem.

In Digital Ethiopia 2030, cybersecurity is acknowledged as a key precondition for safeguarding digital government systems, citizen data and national critical infrastructures. Increased institutional dependency and digital exposure with the interconnected systems escalate cyber security concerns like phishing attacks, ransomware, insider threats, API vulnerabilities, and data breaches. The Mesob ecosystem enables the implementation of the cybersecurity goals in digital governance by embedding secure interoperability frameworks, context-aware security mechanisms, identity and access management systems, Zero Trust Architecture, continuous monitoring systems, and threat intelligence capabilities in the digital governance space.

In addition, two other strategic fields are significant: artificial intelligence (AI) and data governance, both of which are also part of DE2030. Data governance frameworks provide government and citizen data with secure management, classification, protection and exchange, based on the common regulatory and security requirements. AI and data governance mechanisms enable evidence-based governance, secure data exchange, institutional coordination and real-time optimization of digital services within the Mesob ecosystem.

The Citizen-Centered Digital Services is another key element of Digital Ethiopia 2030. The main thrust of the strategy is to enhance public access to government services that are integrated, delivered through centralized digital platforms and interoperable systems. Citizens can now access a range of public services including identification, taxation, licensing, immigration, healthcare and financial services from a single digital environment in the Mesob Digital Collaboration Ecosystem.

Modernization of the digital economy is also a key action of the DE2030 strategy. Ethiopia's vision is to build up digital financial systems, electronic commerce, innovation ecosystems, fintech platforms and technology-based economic activities to foster sustainable national development. The Mesob ecosystem helps achieve this goal by providing secure and reliable digital transactions, financial service interoperability, trusted digital infrastructure, and financial institutions collaboration.

The Mesob Digital Collaboration Ecosystem is the operational framework and platform that enables the implementation of the goals of Digital Ethiopia 2030 in terms of digital governance practices. It allows for the secure interoperability of government systems, institutional coordination, sharing of digital infrastructures, and citizen-centered service delivery. The Mesob ecosystem facilitates Ethiopia's shift towards a modern, secure, resilient, and digitally empowered national governance ecosystem by linking digital governance frameworks through cybersecurity mechanisms, AI technologies, cloud infrastructures, and secure identity management. The two foundations are Digital Ethiopia 2030 (Strategic Foundation) and Mesob (Operational Foundation).

- Digital Ethiopia 2030 (DE2030) is the national programme and strategy for digital transformation in Ethiopia and Mesob Digital Collaboration Ecosystem is the operational platform for leveraging integrated digital governance and institutional collaboration.
- The DE2030 strategy emphasizes the following pillars: digital governance, digital infrastructure, cybersecurity, artificial intelligence, data governance, citizen-centered digital services and modernization of the digital economy.
- The Mesob ecosystem serves as a platform for government institutions to connect securely, exchange data in real-time, deliver services seamlessly, and communicate effectively with one another, supported by technologies like cloud computing, digital identity systems, APIs, and centralized authentication methods.
- Cybersecurity is indeed a key part of DE2030 and Mesob ecosystem, encompassing Zero Trust Architecture, Identity and Access Management (IAM), constant monitoring, secure interoperability and threat intelligence to fortify cyber resilience and safeguard critical digital infrastructures.

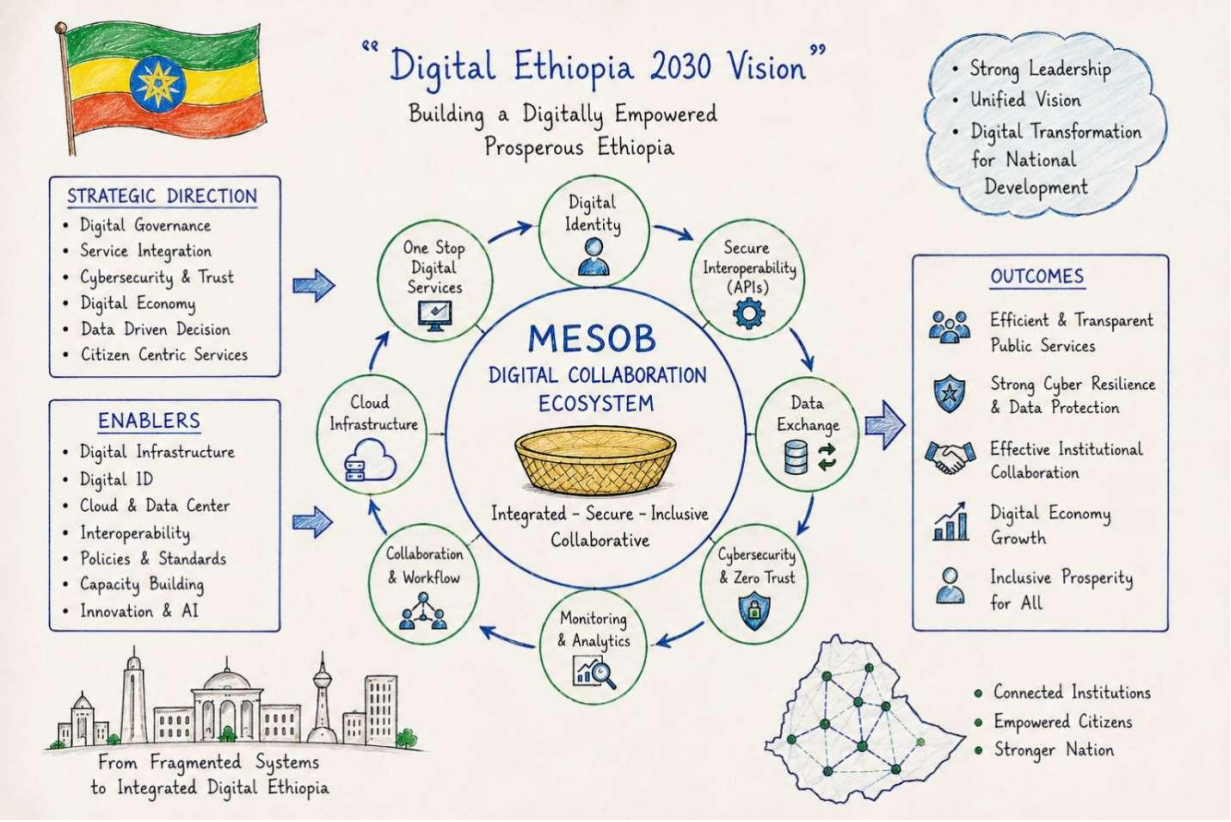

Figure 1: Digital Ethiopia 2030 as Strategic Foundation and Mesob as Operational Foundation

2.2 Digital Ethiopia 2030 Strategy and Cybersecurity Initiatives

The Digital Ethiopia 2030 (DE2030) Strategy is Ethiopia's national plan for digital transformation that aims to boost socio-economic development through information and communication technologies (ICTs), digital innovations, and digital integration of governance. The strategy focuses on four key areas – modernization of public services, the development of digital infrastructure, institutional efficiency, and digital inclusion – with the objective of supporting the development of a secure and sustainable digital economy.

One of the key goals of the strategy is to transform the public administration by providing interoperable e-government systems and integrated digital platforms. DE2030 encourages digital services that are citizen-centric and empower government entities to share information efficiently, coordinate and minimize administrative fragmentation. Citizens can access various services online via a single digital platform, as part of integrated digital governance.

It also lays emphasis on the development of national digital infrastructure namely broadband connectivity, cloud computing environments, national data centers, mobile communication systems, digital payment systems, and national digital identity platforms. These infrastructures are the technological pillars of digital governance, e-commerce, financial access and secure digital communications.

Cybersecurity has also taken center stage within the Digital Ethiopia 2030 agenda, alongside digital transformation goals. With more and more interconnected systems, cloud platforms, APIs, mobile applications, and shared infrastructure to rely on, Ethiopia is becoming more vulnerable to cyber threats like cyberattacks, ransomware, data breaches, identity theft, insider threats, cyber espionage, and attacks against critical national infrastructure.

To address these challenges, the DE2030 strategy includes several cybersecurity initiatives, which will support the creation of a more resilient cyber environment for the country and also safeguard digital ecosystems. A critical project is creating national cybersecurity governance systems, which will include policies and standards, laws and regulations, and institution responsibilities for securing digital systems and information assets in the public and private sectors.

The strategy also supports the implementation of national digital identity and identity and access management (IAM) systems in order to enhance the

authentication, authorization and secure access control mechanisms to digital services. These systems support the mitigation of unauthorized access, identity fraud and account compromise in digital platforms.

A key cyber security effort is the creation of Security Operations Centers (SOCs) and ongoing monitoring to rapidly discover, analyze and react to cyber risk. These systems can be used to facilitate threat detection, incident response, vulnerability management, and cyber threat intelligence sharing between institutions. DE2030 also underscores the enhancement of critical information infrastructure, such as telecommunications, financial, national database, cloud and government platforms. This includes introducing cybersecurity risk management processes, disaster recovery processes, backup, encryption, and business continuity planning to guarantee service availability and operational resilience.

The strategy further helps promote the use of secure cloud architectures, API security frameworks, data protection mechanisms and secure interoperability standards for integrated digital ecosystems like the Mesob Digital Collaboration Ecosystem. These measures are crucial to supporting interrelated systems to exchange data, integrate workflows and collaborate among institutions.

Ethiopia's cybersecurity activities under DE2030 also include cybersecurity awareness campaigns and capacity development initiatives to enhance digital literacy, cyber hygiene, and professional cybersecurity skills for government officials, institutions, businesses and citizens. Training programs, cyber security education and the development of the technical workforce have been identified as key factors in developing sustainable national cyber defense capabilities.

The approach also seeks to strengthen national capacities for responding to cyber incidents and prevent cybercrime at the national level by fostering cooperation between government bodies, law enforcement, telecom companies, financial institutions and regulators. This joint effort will increase national capability in the face of new threats on the internet and facilitate coordinated responses to internet security incidents.

Additionally, DE2030 advocates for the incorporation of new and advanced cybersecurity technologies, such as AI-driven threat detection, adaptive security solutions, behavioral analytics, zero-trust security, and context-aware cybersecurity principles, which will strengthen Ethiopia's digital landscape.

In summary, the Digital Ethiopia 2030 Strategy is not just about digital transformation and economic modernization; it also acknowledges the importance of cyber security as a prerequisite for a secure digital governance, trust in the institutions, digital resilience, and sustainable national development.

- **Digital Ethiopia 2030 focuses on digital transformation and E-Governance:** It is aimed at the modernization of government services through integrating e-government platforms, interoperable systems and citizen-oriented digital services in order to enhance efficiency, transparency and public service delivery.
- **Enhancing National Digital Infrastructure:** The strategy prioritizes building broadband infrastructure, national data centers, cloud computing, digital payments, mobile communication networks and digital identity platforms to enable Ethiopia's digital economy and ensure digital governance.
- **National Cybersecurity Governance and Protection:** DE2030 emphasizes cybersecurity through National cybersecurity frameworks, policies, standards, regulatory mechanisms and institutional governance structures for the protection of digital systems, data and critical national infrastructure.
- **Identity and Access Management (IAM) and SOC Initiatives:** The plan supports the development of secure identity systems and identity and access management (IAM), Security Operations Centers (SOCs), continuous monitoring, threat intelligence, and incident response strategies to further build national cyber resilience.
- **Advanced Cybersecurity and Capacity Building:** Digital Ethiopia 2030 aims at promoting the use of advanced cybersecurity technologies like AI-powered threat detection, Zero Trust Architecture, adaptive security, secure cloud computing, API security, and cybersecurity awareness and capacity building programs to propel sustainable digital transformation.

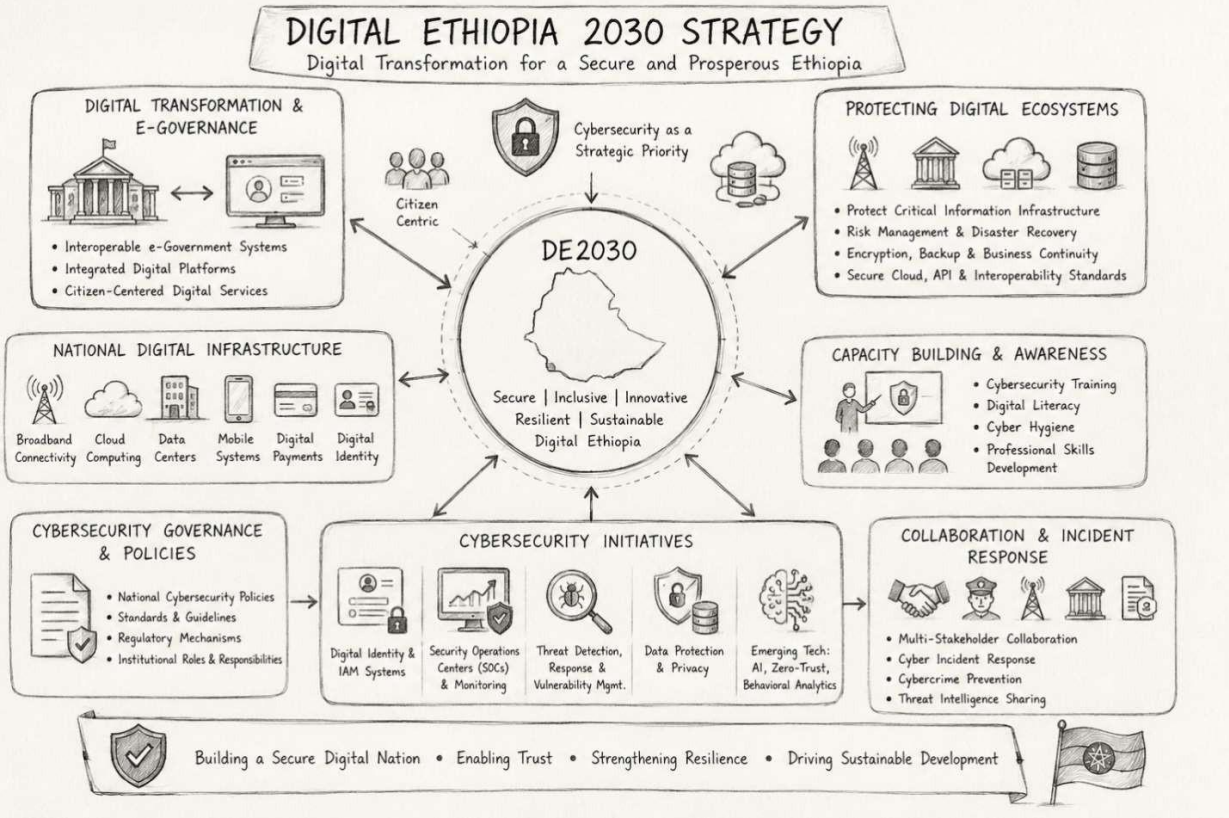

Figure 2: Digital Ethiopia 2030 Strategy and Cybersecurity Initiatives

2.3 Mesob Digital Collaboration Ecosystem

The Mesob Digital Collaboration Ecosystem is a digital governance framework developed as part of the Digital Ethiopia 2030 (DE2030) Strategy with the aim of facilitating collaborative, interoperable, secure, and integrated work between government institutions, citizens, and private organizations. It is a move away from the multiple and silo mentality of digital systems to one national digital architecture that will enable coordinated service delivery, data sharing and real-time interaction between institutions.

The term “Mesob” has its origin in the traditional woven basket in Ethiopia that was used to hold the community's meals, representing unity, sharing, inclusiveness and collective participation. In the digital world, the cultural metaphor is recreated to signify a shared digital space where several actors are able to access, share and control information and services in a interconnected way. For this reason, the Mesob ecosystem is designed to be an integration layer for many different institutions and not as a single application itself, thus allowing for interoperability between the various digital platforms.

From a technical perspective, the Mesob Digital Collaboration Ecosystem integrates various components such as digital identity systems, API-based interoperability frameworks, centralized authentication services, shared data exchange platforms, and workflow integration mechanisms. They enable communication between various government organizations and agencies, data interoperability and real-time coordination of service delivery. The ecosystem is related to horizontal integration (between institutions at the same administrative level) and vertical integration (between federal, regional and local governance levels).

To facilitate citizens' interactions with several e-government services through a single point, the ecosystem is crucial for improving the delivery of e-government services. Users can use one digital interface to access multiple services, such as identification, taxation, immigration, licensing, civil registration, and social services instead of using multiple systems to access each of the services. This leads to more efficient services, less duplication in services and a better experience for users.

One of the primary tenets of the Mesob Digital Collaboration Ecosystem is “interoperability,” meaning the ability for disparate systems built by different institutions to be able to communicate with each other and share information. This is done by standard APIs, data governance polices, shared digital

infrastructure, and a common authentication protocol. Interoperability is critical to break down institutional barriers and to achieve integrated digital governance. With the highly interconnected nature of the Mesob ecosystem, Cybersecurity is also a basic need of the ecosystem. The distributed nature of multiple institutions sharing data and services means the ecosystem must provide confidentiality, integrity, availability and trust. This requires the adoption of robust systems for identity and access management, encryption, secure communication channels, and ongoing monitoring and surveillance to reduce cyber risks.

Moreover, the Mesob ecosystem promotes data-driven governance by allowing for data collection, integration, and analysis from various sources. This facilitates evidence-based decision making, policy making, and performance monitoring at government institutions. It also promotes transparency and accountability in government.

The technical integration is not enough; strong institutional coordination and governance are needed in the ecosystem. This involves defining roles and responsibilities, signing data-sharing agreements, enforcing regulatory compliance and aligning with national digital policies under DE2030. Good governance is critical for keeping ecosystem trust, accountability and sustainability.

In summary, the Mesob Digital Collaboration Ecosystem is one of key components of Ethiopia's digital transformation. It helps to achieve integrated digital governance, enhance institutional cooperation, enhance public service delivery, and facilitate the transition towards a single, secure and interoperable national digital system that meets the goals of the Digital Ethiopia 2030 Strategy.

2.4 Era of Digitalization and Ethiopian Prime Minister’s Aspiration

Digitalization is the global transformation where traditional, paper-based and fragmented systems are replaced by integrated, data-driven and technology-enabled digital ecosystems. It is happening due to progress in information and communication technologies (ICTs), cloud computing, artificial intelligence, mobile technologies and interoperable platforms that facilitate real-time communication, automation, and data-driven decision making across all sectors of society.

Digitalisation is closely associated with the vision of Ethiopia's national development to build a digitally empowered economy and society as envisioned by the Digital Ethiopia 2030 (DE2030) Strategy, which has been in the country's development agenda for a long time. The national development vision of the country, the Prime Minister's national development aspiration, is a strong endorsement of this strategy as it puts modernization, innovation, and digital transformation as cornerstones of the development path Ethiopia is taking.

The Ethiopian Prime Minister's vision of digitalization places emphasis on the vision of an "Ethiopia a knowledge-based economy" through the use of modern governance systems, the development of digital infrastructure, better service delivery and the inclusive access to digital technologies. This vision focuses on the role of technology to increase transparency, to boost institutional efficiency, to foster economic development and to deliver better public services to citizens. It is also a part of a larger vision for Ethiopia's digital economy to become a competitor in the African continent.

Historically, the Ethiopian public administration was poorly equipped with ICTs and the system was still largely paper-based with institutional systems that were not integrated. Through the national leadership of the current digital transformation agenda, efforts are made to address these challenges by fostering digital governance, interoperability and decision-making processes based on data. This shift is planned to promote efficiencies in administration, coordination between institutions, and citizen-service oriented delivery of services.

The cultural concept of unity and collective participation “Mesob,” which is central in Ethiopia, is a hallmark of the national aspiration, echoed in the establishment of a Mesob Digital Collaboration Ecosystem. In this digital environment, the ecosystem is a single, secure, interoperable, and integrated digital environment where citizens, private organizations, and government institutions interact. It represents the leadership goal of a national digital infrastructure that is connected and collaborative.

Broadband expansion, mobile connectivity, the deployment of cloud computing systems, national data centers, and digital identity platforms are other major investments in digital infrastructure that are helping to support the digitalization era in Ethiopia. These core systems are critical to providing scalable e-government services, digital financial systems, and a financially innovative economy. But impediments like infrastructure deficits, cybersecurity concerns, digital skills deficits and the urban-rural divide remain to impact the pace and equity of transformation.

The Ethiopian Prime Minister's vision, from a strategic point of view, not only involves technological development but also the reform of institutions and socio-economic transformation. It has envisioned an efficient, transparent and citizen-centric government system, private sector involvement and digital entrepreneurship. The ability to incorporate cutting-

edge technology like AI, big data analytics, and secure digital identity systems only adds to this vision's future potential.

To sum up, digitalization in Ethiopia is a transformation process that is driven by the national agenda, has high political buy-in and is defined by the Digital Ethiopia 2030 Strategy. The Prime Minister's vision also highlights digital transformation as a key pillar of Ethiopia's development trajectory, and the Mesob Digital Collaboration Ecosystem is one of the mechanisms that helps implement this vision in a country-wide way through digital governance that is integrated, secure, and collaborative. Era of Digitalization and Ethiopian Prime Minister's Aspiration is

- **Digital Transformation and Modernization:** An era of digitalization is the world's transition from legacy manual processes to a digital world that incorporates ICT, cloud computing, artificial intelligence and data-driven solutions for efficient governance and service delivery.
- **Digital Ethiopia 2030 Vision:** Ethiopia's Digital Ethiopia 2030 (DE2030) Vision is to create a digitally empowered economy and society through modern digital infrastructure, innovation, e-government services and inclusive digital access.
- **Prime Minister's National Aspiration:** The Ethiopian Prime Minister's vision is the Prime Minister's National Aspiration, which aims to shift the economy of Ethiopia towards being knowledge-based and technology-driven, by enhancing transparency, the efficiency of institutions and the government's digitalization, and delivering citizen-driven public services.
- **Mesob Digital Collaboration Ecosystem:** The Mesob ecosystem embodies national unity and collaboration by establishing a secure, interoperable and integrated digital platform, which can link government institutions, private sectors and citizens through digital platforms.
- **Cybersecurity and Sustainable Digital Development:** Ethiopia's digital transformation agenda puts a high priority on building resilient digital infrastructure, cybersecurity, developing digital identity systems, implementing AI and digital skills training, and ensuring sustainable economic development through digital solutions while safeguarding national digital governance.

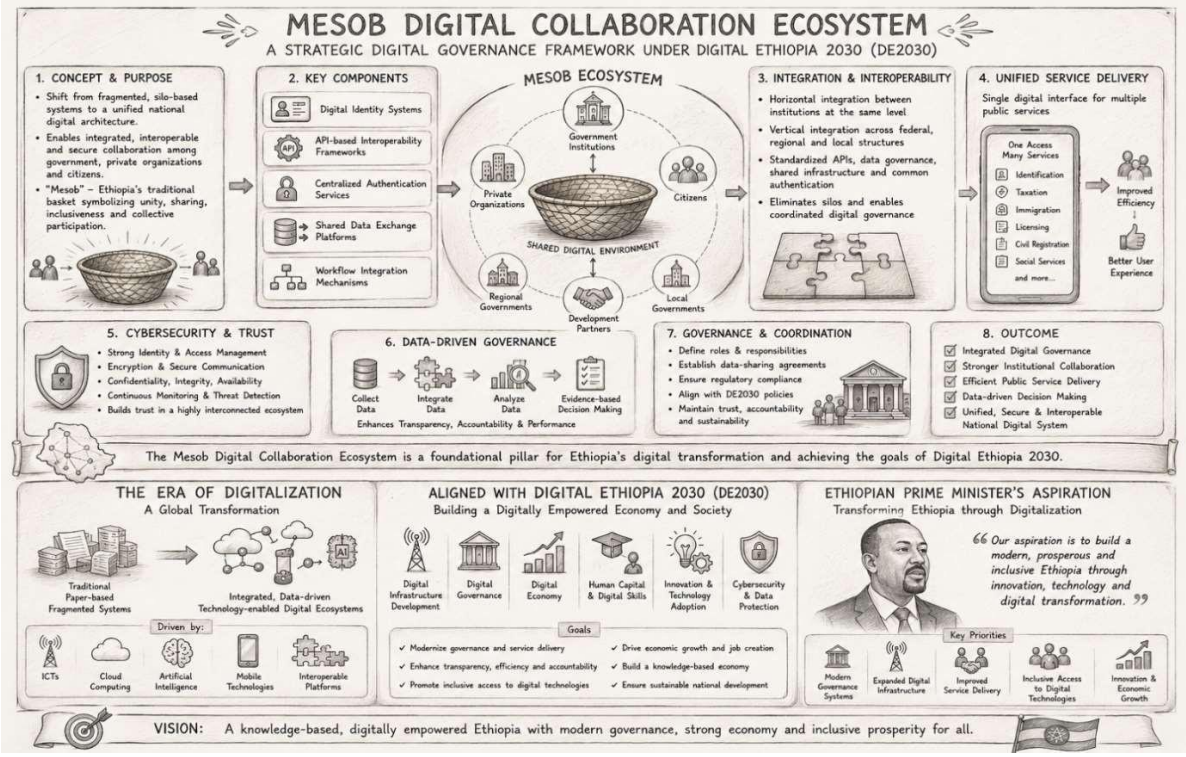

Figure 3: Era of Digitalization and Ethiopian Prime Minister's Aspiration

2.5 Comparative Analysis: Ethiopia's Digitalization and Resilience in the African Context

In the context of the continent's drive towards digitalization, Ethiopia is making significant strides towards digital transformation under the Digital Ethiopia 2030 (DE2030) Strategy. Like Rwanda, Kenya, and South Africa, Ethiopia is on the way to investing in digital governance, cloud-based systems,

digital identity systems and interoperable government platforms. However, Ethiopia still has several issues pertaining to cybersecurity maturity, institutional coordination, infrastructure limitations and interoperability security. The Mesob Digital Collaboration Ecosystem is a pioneering Ethiopian model of collaborative, inclusive and secure digital governance. While significant strides have been made, the country is still facing challenges in digital transformation, such as a need for more effective cybersecurity governance, context-aware security frameworks, and resilient digital infrastructure, as well as the need for trained manpower.

2.5.1 Digitalization and its impact on the Ethiopian private sector

Disparities in maturities across Africa are great, reflecting differences in infrastructure development, policy landscape, innovation ecosystem, and institutional capacity. Countries like Kenya, Rwanda, Nigeria and South Africa are known to be among the best digital economies owing to their highly developed e-government platforms, robust fintech ecosystems and well-established digital infrastructure.

Ethiopia is in the process of a systematic and planned digital transformation based on the country's Digital Ethiopia 2030 (DE2030) Strategy, which focuses on integrated digital governance, interoperability, and digital development in an ecosystem approach. In this context, the Mesob Digital Collaboration Ecosystem is a core project to support institutional linkages, data sharing and coordinated delivery of digital services within the government sector. Ethiopia has advanced strategically, but is still in a transitional phase to achieving digital ecosystem maturity. There are remaining gaps in interoperability depth, private sector involvement, innovation ecosystem development and cybersecurity maturity when compared to the leaders of the African continent. But, Ethiopia's long-term strategic approach, which is centralized, has set a good framework for future digital resilience.

2.5.2 Digital Infrastructure and Connectivity Development

The telecom sector has been limited and uncompetitive in Ethiopia, and this framework has historically been the driver for the development of Ethiopia's digital infrastructure. This architecture limited innovation, service proliferation and network reach for many years. New reforms such as partial liberalization of the telecom sector and the introduction of new operators, however, have greatly enhanced connectivity, the flow of investment and service quality.

Significant progress has been made in the rollout of the 4G network, in the early deployment of pilot 5G networks, and in the preparation of the national fiber optic backbone to enable high-capacity data communications. Furthermore, government investments in data centers and cloud infrastructure are improving the underpinnings for e-government services and digital ecosystems like Mesob. Internet usage has been slowly increasing, but is still lower than that of the top digital economies in Africa.

However, there remain some challenges, such as the lack of quality, affordable, and widespread Internet connectivity between rural and urban areas, a lack of infrastructure redundancy, and the continued use of centralized systems. Ethiopia's infrastructure is still in the growing stage and is gradually improving, when compared to Kenya, Rwanda, South Africa and Nigeria. The resilience of its digital dimension is moderate and steadily improving.

2.5.3 Digital Governance and E-Government Maturity

DE2030 is enabling a shift from disjointed e-government approaches in Ethiopia to a coordinated digital governance approach. In the past, government institutions worked in silos with isolated systems, and these had not been interoperable, resulting in inefficiencies, duplication of services and poor coordination.

The Mesob Digital Collaboration Ecosystem marks a major step towards integrated governance. It allows for interoperability among institutions, sharing of infrastructure, and a coordinated service delivery. Data exchange mechanisms are being put in place at the early stage between key government agencies and at one-stop service centers, to link identification, tax, immigration and licensing services.

Despite all of this, there are still some drawbacks to consider, such as using outdated technology, workflows that are not fully automated and an overall lack of real-time data sharing among institutions. Ethiopia's governance systems are in an early to intermediate stage of e-government maturity, significantly behind Rwanda's highly integrated e-government system, Kenya's centralized service portal, and South Africa's advanced but complicated governance systems. However, its centralized integration strategy offers great promise for future system-wide coordination and resiliency.

2.5.4 Digital Economy and Financial Technology Ecosystem

The digital economy is at an emerging phase in Ethiopia with the slow process of modernization of the financial sector under the DE2030 framework. The country has advanced in mobile banking dissemination, digital payment mechanisms, and linking up telecommunications and financial services. Government-backed digitization of financial services, such as electronic tax systems and electronic payment platforms, is also helping to drive economic change.

But the fintech sector is still not as developed as other African countries. The startup landscape is underdeveloped, the economy heavily cash-centric, and the regulatory climate is composed of a mix of conservative and stable regulations with a financial stability as their primary concern that does not welcome fast-paced innovation. By contrast, Kenya is a leader in mobile money innovation, Nigeria has the continent's biggest fintech start-up hub and South Africa has a well-developed and regulated digital banking industry.

The financial digital ecosystem is relatively stable, though slow growing in Ethiopia, from a Resilience point of view. Both regulatory control and innovation and financial inclusion are key to its long-term competitiveness.

2.5.5 Cybersecurity and Digital Risk Management

Cyber security in Ethiopia is still at an early stage but is becoming an important component in the DE2030 strategy. With the growing interconnection of digital systems, cyber security threats like ransomware, data breaches, insider risks and infrastructure attacks are rising.

National efforts involve establishing cybersecurity governance structures, enhancing institutional security measures, embedding security in digital identity systems like Fayda, and capacity building in incident response and cyber defense. These efforts focus on improving the nation's cyber resilience and safeguarding critical digital infrastructure.

However, the efforts have not been without hurdles, such as lack of qualified cybersecurity workers, disjointed institutions' security policies, and inadequate systems for detecting and responding to incidents. Ethiopia's cybersecurity maturity is still in its early stages, when compared to South Africa and Kenya. The continued embedding of cybersecurity into national platforms like DE2030 and Mesob, however, is a positive step toward increased resilience.

2.5.6 Digital Identity and Data Governance Systems

Fayda is an integral part of Ethiopia's digital transformation strategy. It gives citizens a unique digital identity that can be used to authenticate at various government and private sector platforms in a secure way. It also helps with interoperability across the Mesob ecosystem and eliminates duplicate identity and fraud.

Nevertheless, the system is still expanding, and efforts are continuously underway to expand coverage, integration and institutionalization. Data governance systems are also being enhanced to provide privacy, security and controlled data sharing between institutions.

The identity ecosystem in Ethiopia is in a development phase, as compared to Rwanda's largely integrated national identity system, Kenya's developing digital identity system, and South Africa's well-established civil registration system, and includes strategic importance for future digital resilience and integration of services.

2.5.7 Ecosystem Integration and Interoperability

The Ethiopia Digital Collaboration Ecosystem (Mesob) is one of the key innovations in National Digital Governance. It aims for API-based interoperability, standardized services, cross-ministerial data sharing, and single integration architecture. This allows previously "siloed" systems to connect and work together in one digital space.

Ethiopia is developing interoperability at the very core of its architecture, as opposed to many countries in Africa where integration would be layered on top of existing disjointed architectures. It will increase system resiliency, control from governance and scalability.

2.5.8 Overall Digital Resilience Assessment

Digital resilience is the capacity of a digital ecosystem to resist, adapt and bounce back from disruptions. The digital resilience of Ethiopia is promisingly emerging but structurally.

The key strengths are good policy coordination at the central level under DE2030 on a number of policies, development of the interoperability of the Mesob ecosystem, progress in the development of the Fayda digital identity system, and continued liberalization of the telecom sector. These factors all contribute to a more robust institutional coordination, service integration and digital governance stability over time. There is, however, a number of challenges that could be identified, such as low level of infrastructure redundancy, low cyber security maturity level, lack of qualified ICT professionals and reliance on centralized systems. Ethiopia is at a transitional stage, still moving towards a positive trajectory, relative to the top African digital economies.

Overall, the national strategies are beginning to build digital resilience, with an increasing focus on integrating the digital ecosystem and developing infrastructure in Ethiopia. Complete maturity will be achieved through ongoing development of cybersecurity capacity, interoperability growth, infrastructure diversification and digital skills enhancement.

2.5.9 Citizen-Centered Digital Services

One of the key priorities of the Digital Ethiopia 2030 (DE2030) Strategy and Mesob Digital Collaboration Ecosystem is the development of Citizen Centered Digital Services. The rationale for these services is to address the problems of inaccessibility, inefficiency, lack of transparency and inconvenience faced by citizens in their interactions with government and

government institutions by providing integrated digital services and platforms instead of disjointed and isolated services. It is about putting citizens at the heart of digital governance, making it easier to access services and smooth to use the services provided by public institutions.

Mesob Digital Collaboration Ecosystem's integration allows citizens to use various government services through one single digital platform. Users do not have to switch between different institutional processes for taxation, identification, licensing, immigration, health services, and financial transactions, but can access them in a seamless and interoperable process. This integration streamlines administrative processes, curbs duplication of effort, and enhances the effectiveness of Public Service delivery.

The interoperability is a key element of the Mesob ecosystem's citizen-centric nature of digital services. Different government systems created by various ministries and agencies are connected via APIs, common digital infrastructure and established communication channels. This interoperability allows for the secure exchange of data and coordinated delivery of services between institutions, thus increasing the speed and uniformity of digital services to citizens. It also eliminates the need for the repeated submission of documents and manual verification, enhancing operational efficiency and user satisfaction.

Digital identity systems are essential for citizen-centric digital services, providing a means for authentication and access management across various government platforms. National digital identity systems enable citizens to access various public services in a secure manner with a single verified identity. The central authentication system increases trust, enhances identity verification, decreases fraud, and makes user access to digital government services easier. Security within the ecosystem is further bolstered by integration of Identity and Access Management (IAM) mechanisms, Multi-Factor Authentication (MFA) and secure authentication protocols.

Digital payment systems can also facilitate citizen-centered service delivery, allowing citizens to make secure financial transactions online through government platforms. Electronic payment options for citizens for taxes, licensing fees, utilities and other government services are possible without having to make a physical trip to the government offices. Digital payment systems create better financial inclusion, faster transactions and better transparency for government finances. The systems also enhance the development of Ethiopia's digital economy and assist the overall digital transformation projects under DE2030.

In addition, citizen-oriented services play a key role in transparency, accountability and institutional modernization. Digital platforms that integrate platforms enhance the monitoring function, minimize bureaucratic inefficiencies, and facilitate data-driven governance. Geographic access to services for citizens is improved, especially in the context of digital services supported by mobile technologies, cloud infrastructure and national connectivity infrastructure.

Even with these benefits, there are a few obstacles in the way of implementing citizen-centered digital services in Ethiopia. These encompass limited digital infrastructure in rural areas, lack of interoperability between institutional systems, cybersecurity threats, digital literacy deficiencies, and security controls implementation issues of government platforms. What is needed to address these challenges are better cybersecurity governance, better digital infrastructure, institutional coordination and ongoing investments in cybersecurity technology and development that are secure and inclusive.

Citizen-oriented digital services in the Mesob Digital Collaboration Ecosystem contribute to the shift towards an integrated digital governance in Ethiopia by enhancing the accessibility, interoperability, efficiency and trust of public service delivery. The ecosystem is part of reaching the vision of the Digital Ethiopia 2030, which is the transition to a modern, inclusive, and digitally empowered society, through a unified digital identity system, interoperable platforms, and secure digital payment infrastructure.

2.5.10 Secure, reliable, and scalable shared digital infrastructure and cybersecurity

The technology backbone of Ethiopia's Digital Ethiopia 2030 (DE2030) Strategy and the Mesob Digital Collaboration Ecosystem is shared digital infrastructure. It provides a framework for the government institutions, digital platforms and public services to function in an integrated, interoperable and coordinated digital environment. With Ethiopia moving towards digital governance and data-driven public service, shared digital infrastructure that is effective and secure is vital to ensure service continuity, operational efficiency, and national cyber resilience.

The adoption of the Mesob Digital Collaboration Ecosystem is highly reliant on the different infrastructure components that are interlinked, such as national cloud systems, government data centers, secure APIs, national communication networks, digital identity systems and shared integration platforms. Together they enable the delivery of digital services, inter-institutional cooperation, secure data exchange and citizens' engagement in digital governance.

Cloud systems offered by National/Provincial entities are a scalable and centralized computing solution that enables the hosting, storage, processing and management of government applications and digital services. Cloud infrastructure facilitates the sharing of resources in an efficient manner, thereby cutting down on cost of operations and increasing the availability of services. Cloud environments also pose cybersecurity threats like unauthorized access, improper configurations, multi-tenancy vulnerabilities, and data leakage. Thus, good cloud security governance, encryption, identity management and ongoing monitoring is important to secure government cloud infrastructures.

Government data centers are vital resources for the national database, the digital government platform and institutional applications. These data centers are important facilities for storing and processing highly sensitive information related to government and citizens, and are therefore high-value targets for cyberattacks. Physical and logical security of government data centers is a crucial component in the security of digital services to ensure confidentiality, integrity and availability. This can involve access controls, backup systems, disaster recovery plans, environmental controls, and ongoing monitoring and security measures.

Secure APIs (Application Programming Interfaces) are at the heart of interoperability and communication among interconnected systems in the Mesob ecosystem. APIs enable government bodies to share data and synchronize services in real time. But if API authentication, authorization and encryption are not as strong as they should be, they can turn into a significant attack vector. Digital integration platforms need to be secured against unauthorized access and cyber threats with a range of cybersecurity measures including: Secure API gateways, Token-based authentication, Encrypted communication channels, API monitoring, and Access control policies.

National communication networks are the connectivity infrastructure that is needed for digital government operations, cloud communication, internet access, and institutional coordination between federal and regional levels. They encompass mobile telecommunication networks, broadband networks, internet backbone (backbone) networks, and government intranet networks. National networks are key to digital governance, and cybersecurity measures like network segmentation, intrusion detection systems, firewalls, secure routing protocols, and traffic surveillance are essential for ensuring the network remains resilient and able to withstand cyber-attacks and service disruptions.

Another key element of shared digital infrastructure is digital identity systems. These systems can be used to facilitate secure authentication, identity verification, and access management in government services. Citizens and government workers can access several digital platforms with a single authentication process, ensuring secure access to digital platforms. The integration of Identity and Access Management (IAM), Multi-Factor Authentication (MFA), biometric authentication and context-aware authentication are essential in enhancing cyber security across the digital landscape and mitigating identity fraud and unauthorized access risks.

Shared integration platforms offer the interoperability layer between ministries and agencies, regional institutions and digital government services. These platforms facilitate synchronised workflows, safe information sharing and consolidated service provisioning among institutions. Integration platforms not only simplify communication and data flows, they also add man-made complexity to cyber security as well as a larger attack surface. Therefore, robust cybersecurity governance, secure interoperability standards, Zero Trust Architecture, continuous monitoring systems and centralized threat intelligence are essential to ensure the safety of interconnected systems and the trust of the ecosystem.

Cybersecurity is an essential part of the assurance and sustainability of common digital infrastructure. The more complex and interdependent the government systems, the more likely that one weakness in one system may impact several institutions and critical services. Thus, a comprehensive cybersecurity strategy, incorporating all layers of infrastructure from preventive, detective and responsive controls, is needed to support Ethiopia's digital transformation.

To secure a shared digital infrastructure in the Mesob ecosystem, there are multiple cybersecurity measures that must be taken. They cover encryption solutions to secure data in transit and at rest, Security Operations Centers (SOC) for centralized monitoring, Security Information and Event Management (SIEM) systems for log analysis and threat detection, Zero Trust security models for ongoing verification, and incident response tools for quick incident containment. Furthermore, context-aware security mechanisms, behavioral analysis, and AI-driven threat detection can provide additional layers of security against ever-changing cyber threats.

While the country has made strides, there are still a few issues to be addressed when it comes to shared digital infrastructure and cyber security in Ethiopia. These include lack of infrastructure maturity and inconsistent implementation of security in institutions, a lack of trained cybersecurity professionals, lack of

redundancy and disaster recovery capability, budget limitations, and digital connectivity gaps between urban and rural areas. Improved governance, institutional coordination, ongoing investment of cybersecurity technologies and alignment of infrastructure development and national cybersecurity strategies are necessary to overcome the challenges. In summary, the shared digital infrastructure is the backbone of Ethiopia's digital transformation agenda and the Mesob Digital Collaboration Ecosystem. The convergence of cloud systems, government data centers, APIs, communication networks, digital identity systems, and interoperability platforms in a secure cybersecurity environment will not only help with the successful implementation of the Digital Ethiopia 2030 vision but also contribute to digital governance, better service delivery, better institutional collaboration, and overall better cybersecurity.

- **Shared digital infrastructure:** The shared digital infrastructure of Ethiopia is the backbone of the Digital Ethiopia 2030 and Mesob ecosystem, facilitating integrated digital governance, secure data sharing, interoperability, and citizen-centric public services through cloud systems, data centres, APIs, communication networks and digital identity platforms.
- **Cybersecurity is essential:** In order to safeguard connected government systems and critical services, a robust cybersecurity capability is needed. Some of the key features are: Encryption, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Zero Trust Architecture, SOC/SIEM monitoring, intrusion detection and secure API management.
- **Major infrastructure components:** The services will be more efficient and collaborative with major infrastructure components like national cloud systems, government data centers, secure APIs, communication networks and shared integration platforms, but they will also bring cyber risks such as "unauthorized access, data leakage, and extended attack surface.
- **Ethiopia faces several challenges:** While Ethiopia grapples with cybersecurity challenges like limited maturity of infrastructure, a lack of cybersecurity professionals, budget constraints, uneven security implementation practices, and poor disaster recovery ability, more cybersecurity governance, investment, institutional coordination, and national cybersecurity strategies are needed.

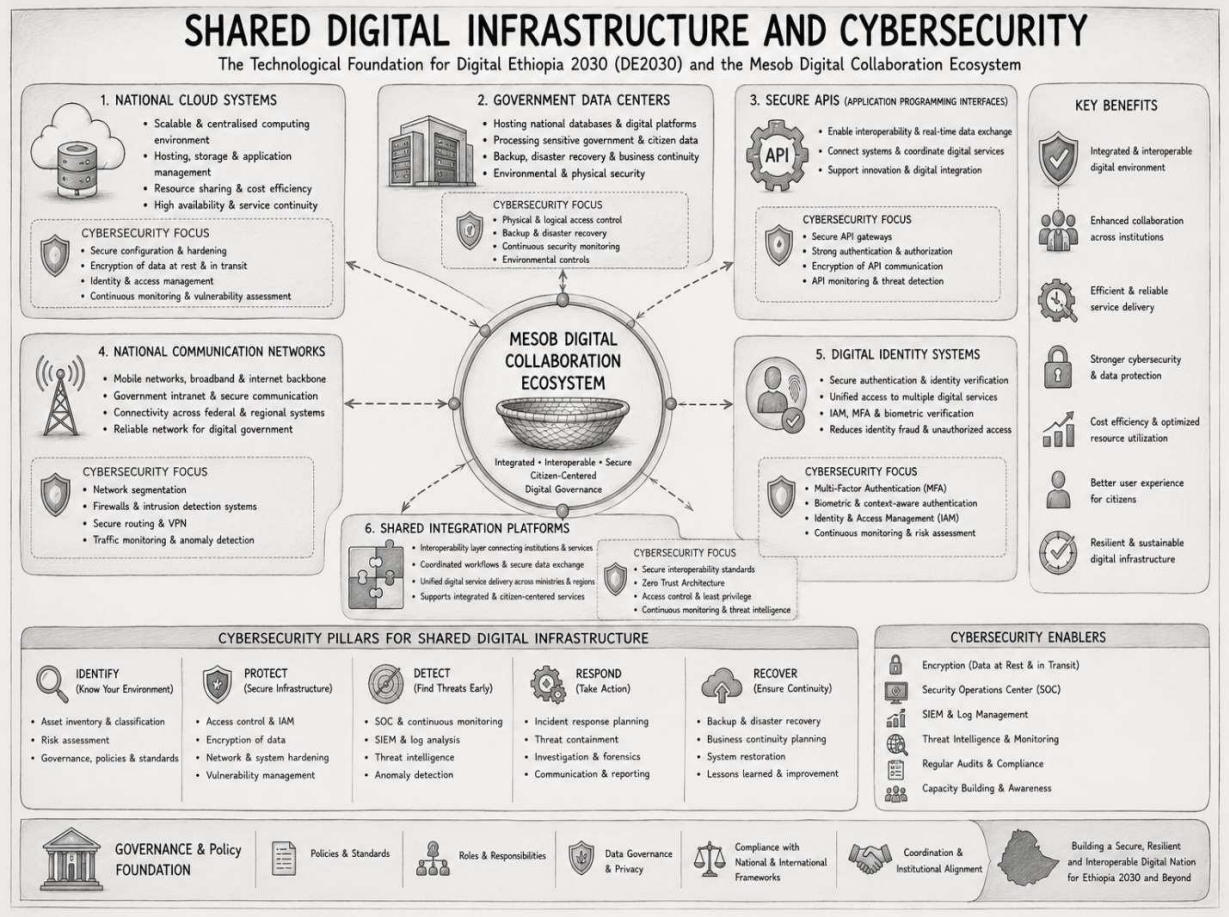

Figure 4, Shared Digital Infrastructure and Cybersecurity

2.5.11 Comparative Analysis of Digital Transformation in Selected African Countries (2025)

As governments increase their capacity to utilize digital infrastructure, e-government platforms, fintech innovation, cybersecurity, and digital identity platforms to enhance governance and public service delivery, digital transformation is quickly gaining momentum in Africa. Countries have made varying progress in digital governance, interoperability and cyber resilience. There are countries like Kenya, Rwanda, Nigeria and South Africa with varying levels of progress in digital governance, interoperability and cyber resilience. Likewise, Ethiopia is making strides towards digital transformation under the Digital Ethiopia 2030 (DE2030) Strategy, digital identity programs, and the liberalization of the telecom sector with the Mesob Digital Collaboration Ecosystem. The comparative analysis provides a snapshot of the status of digital transformation, cybersecurity preparedness, interoperability, and digital resilience of selected countries in Africa, with the aim of drawing key lessons and strategic insights that will be applicable to Ethiopia's digital governance ecosystem.

(Based on ITU, World Bank GovTech, GSMA Mobile Economy, and UN E-Government trends)

Dimension	Ethiopia	Kenya	Rwanda	Nigeria	South Africa
Digital Infrastructure	Ethiopia is undergoing rapid transformation driven by telecom liberalization, expansion of fiber backbone, nationwide 4G coverage, and	Highly developed mobile-driven infrastructure with strong 4G coverage and competitive telecom market.	Strong state-led infrastructure expansion with nationwide fiber connectivity and efficient network deployment.	Large-scale infrastructure base but uneven quality and regional disparities in coverage and service reliability.	Most advanced digital infrastructure in Africa with extensive fiber networks, high

	early-stage 5G pilots. Infrastructure development is strongly state coordination				broadband penetration, and mature telecom markets.
E-Government Systems	Ethiopia is transitioning toward an integrated digital government model through the **Mesob Digital Ecosystem**, which aims to unify fragmented public services into a single interoperable platform. Digital service adoption is increasing across taxation,	Strong citizen-focused e-government system through the **eCitizen platform**, widely used for public services.	One of the most advanced systems in Africa with **Irembo platform**, offering highly integrated and centralized digital government services.	E-government systems remain fragmented across federal and state levels, limiting full integration.	Advanced digital government services exist but are distributed across multiple siloed institutional systems.
Fintech and Digital Economy	Ethiopia's digital finance ecosystem is emerging with regulatory reforms, gradual expansion of mobile money services, and increasing digital payment adoption.	Global leader in mobile money innovation, driven by **M-Pesa**, enabling deep financial inclusion and digital transactions.	Fast-growing digital payments ecosystem supported by strong government policy direction and digital finance adoption.	Africa's largest fintech ecosystem with rapid startup growth, high investment inflows, and strong innovation hubs.	Mature financial system with advanced digital banking services and strong fintech integration.
Cybersecurity	Ethiopia is strengthening national cybersecurity frameworks, establishing institutional capacity, and developing CERT structures.	Established national CERT and growing cybersecurity ecosystem supported by private sector engagement.	Strong cybersecurity governance with proactive national digital security policies.	Cybersecurity systems are improving but enforcement and institutional coordination remain uneven.	Most mature cybersecurity ecosystem in Africa with advanced institutional frameworks and regulatory enforcement.
Digital Identity Systems	Ethiopia is implementing the **Fayda Digital ID system**, which is currently in rollout and scaling phases. It is designed to support national identification,	The **Huduma Namba** system has been partially implemented with ongoing integration challenges.	Fully integrated national digital identity system supporting seamless public service delivery.	Identity systems remain fragmented across multiple registries and institutions.	Mature civil registration system with partial digital integration across services.
Interoperability of Systems	Ethiopia is developing the	Partial interoperability	Highly centralized and	Highly fragmented	Advanced digital

	Mesob API-based interoperability framework, aimed at enabling data exchange across government systems and supporting unified digital service delivery.	exists across selected government platforms but not fully unified.	fully interoperable government digital ecosystem.	systems with limited interoperability across federal and state institutions.	systems exist but are often siloed across departments.
Digital Economy & Innovation	Ethiopia is in a transition phase with growing digital entrepreneurship, policy reforms, ICT sector expansion, and increasing foreign investment in telecom .	Strong innovation ecosystem driven by fintech, mobile services, and technology startups.	Moderate but stable digital innovation ecosystem supported by government-driven programs.	Largest startup and fintech ecosystem in Africa with strong venture capital activity and scale advantage.	Mature digital economy with strong banking, enterprise IT, and service digitization.
Digital Resilience and Governance	Ethiopia is strengthening institutional digital resilience through governance reforms, digital infrastructure expansion,	Moderate-to-strong resilience supported by private sector innovation and mobile ecosystem stability.	High resilience due to centralized governance and coordinated digital transformation strategy		

Table 1, Comparative Analysis of Digital Transformation in Selected African Countries (2025)

African nations are aggressively pursuing digital transformation at a very rapid pace, with significant investment in digital infrastructure, e-government platforms, fintech development, cyber security governance and digital identity platforms. In Kenya, Rwanda, Nigeria and South Africa, digital ecosystems are robust and enable interoperability between government services, digital economies and cyber resilience. Ethiopia is also progressing on its digital transformation journey under the umbrella of the Digital Ethiopia 2030 (DE2030) Strategy by liberalizing telecom services, investing in digital infrastructure, rolling out the Fayda Digital ID system and establishing the Mesob Digital Collaboration Ecosystem.

But there are still cybersecurity maturity, infrastructure, institutional coordination, interoperability security, and digital resilience issues in Ethiopia. The Mesob ecosystem is central to achieving interoperability, security, and citizen-centric service delivery and integrated digital governance. Hence, the need for a context-aware cybersecurity framework to enhance the cyber resilience of Ethiopia, secure its critical digital infrastructure and promote secure and sustainable digital transformation.

- African countries are aggressively pursuing their digital transformation agenda by investing in digital infrastructure, fintech, e-government systems and cybersecurity governance.
- Under the Digital Ethiopia 2030 Strategy, Ethiopia is rapidly making strides towards digital transformation through the Mesob ecosystem, telecom liberalization and digital identity programs.
- Countries like Kenya, Rwanda, Nigeria and South Africa offer comparative examples of digital governance, interoperability and development of digital economy.
- The cybersecurity maturity, infrastructure limitations, institutional coordination and interoperability security problems in Ethiopia are still issues.
- The Mesob Digital Collaboration Ecosystem contributes to the integrated, digital governance, secure interoperability, and citizen-centric public service delivery.
- Strengthening Ethiopia's cyber resilience, digital governance and sustainable digital transformation

requires a framework that is knowledgeable of context (context-aware cybersecurity).

2.6 Problem Statement

Ethiopia is currently undergoing a digital transformation, with tremendous progress in the areas of digital infrastructure, e-government services, cloud computing adoption, and the development of the Mesob Digital Collaboration Ecosystem, under the Digital Ethiopia 2030 (DE2030) strategy. While the cybersecurity capabilities have made significant strides, they have not matched the growth rate of other accomplishments.

Government institutions and services are increasingly connected with each other to a greater degree via application programming interfaces (APIs), cloud platforms, mobile apps, and shared digital infrastructures, which has led to a higher risk of exposure to cyber threats. The growing interdependence has greatly broadened the national cyber-attack surface, with critical systems now being exposed to threats like data breaches, ransomware attacks, unauthorized access and insider threats, as well as the potential for large-scale service disruption. But there is currently no overall, single and contextually relevant cybersecurity framework in place in Ethiopia that enables it to secure its fast-growing digital ecosystem. Current cybersecurity practices still exist at a scattered level between institutions, with only poor coordination, lack of uniformity in standards, information exchange and lack of qualified cybersecurity experts. In addition, national-level incident response and cyber resilience mechanisms are not even proportionate to the size and complexity of current digital transformation.

The challenge is significant in the context of the Mesob Digital Collaboration Ecosystem, which is expected to facilitate interoperability and integrated service delivery within government institutions. However, if it is done without a comprehensive and flexible cybersecurity strategy, it can create new systemic risks, potentially affecting sensitive data, critical public services, and the trust in digital governance structures.

- Ethiopia is embarking on an accelerated digital governance process and on developing interconnected digital services with the strategy of a Digital Ethiopia 2030.
- Cloud systems, APIs, digital identity platforms and shared infrastructures have made the national cyberattack surface bigger and more complex.
- The current cybersecurity practices are siloed, influenced by a lack of governance, standardization, infrastructure, and cybersecurity specialists.
- For the Mesob Digital Collaboration Ecosystem to be able to provide trusted digital governance and secure interoperability, it must be supported by a secure and adaptive cybersecurity framework.
- Ethiopia requires an institutional, technological and socio-economic context-oriented cyber security framework.
- Enhancing cyber security is a vital need to safeguarding critical digital infrastructure, enhancing cyber resilience and enabling sustainable digital transformation.

2.6.1 Core Research Problem

The main research question that will be raised in the study is, therefore:

There is no Cybersecurity framework in Ethiopia that takes into consideration the cybersecurity requirements of the Mesob Digital Collaboration Ecosystem and the interoperability, cyber resilience and trusted digital governance within the framework of the Digital Ethiopia 2030 strategy.

This study has a main research question:

What are the possibilities for building a context-aware cybersecurity framework in Ethiopia that ensures the secure interoperability of its emerging digital ecosystem and the nation's cyber resilience in the context of the Digital Ethiopia 2030 vision?

Addressing this problem is crucial to facilitate secure digital transition, safeguard national critical digital infrastructure and secure the sustained success of Ethiopia's digital government and economy programs.

2.7 Research Objectives

The aim of this research is to create a framework for context-aware cybersecurity to secure Ethiopia' Mesob Digital Collaboration Ecosystem and to facilitate secure, resilient and sustainable digital transformation in the country, under the Digital Ethiopia 2030 (DE2030) strategy.

2.7.1 General Objective

To create an ecosystem-aware cybersecurity framework for the security of the Mesob Digital Collaboration Ecosystem in Ethiopia and its contribution to the national cyber resilience in line with the Digital Ethiopia 2030 strategy.

2.7.2 Specific Objectives

The study has the following specific objectives:

1. **Identify and evaluate** significant cybersecurity threats, vulnerabilities and risks impacting Ethiopia's digital platforms, systems in the cloud, and developing Mesob Digital Collaboration Ecosystem.
2. **To assess** the current cybersecurity governance framework, institutional coordination mechanisms and cybersecurity

management system in the digital government system in Ethiopia.

3. **To assess** the existing cyber security policies, standards, regulations and technical controls concerning interoperable and interconnected digital systems, and identify gaps and challenges.
4. **To establish** a context-aware cybersecurity framework as per Ethiopia's technical infrastructure, institutional environment, regulatory framework, and cultural and socio-context for securing the Mesob Digital Collaboration Ecosystem.
5. **To recommend** adaptive cybersecurity solutions, including risk-based access control, identity and access management, monitoring and continuous monitoring, and threat detection systems, to improve cyber resilience and robust cyber security for digital partnerships.

2.8 Research Questions

The study has the following main and specific research questions:

2.8.1 Main Research Question

What is the way forward for building a context-aware cybersecurity framework in Ethiopia to effectively defend the Mesob Digital Collaboration Ecosystem, to safeguard secure interoperability, and to enhance nation-wide cyber resilience in the context of the Digital Ethiopia 2030 strategy?

2.8.2 Specific Research Questions

1. What are the most significant cybersecurity threats, vulnerabilities and risks to Ethiopia's digital platforms and also the emerging 'Mesob Digital Collaboration Ecosystem'?
2. What is the effectiveness of existing cybersecurity governance, institutional coordination and cybersecurity management practices in Ethiopia's cyber environment?
3. What are the main gaps/challenges in the current Cybersecurity policies, standards, regulations, and technical controls in the context of Interoperable and Cloud based Digital systems in Ethiopia?
4. How to structure a context-aware cybersecurity framework in Ethiopia's technological, institutional, regulatory and socio-cultural context?
5. What adaptive cybersecurity mechanisms (e.g., risk-based access control, identity and access management, continuous monitoring, threat detection) can boost cyber resilience and support digital collaboration?
6. What is the potential of the proposed framework to contribute to the secure digital governance and enhance national Ethiopia cybersecurity readiness within the Digital Ethiopia 2030 vision?

2.8 Significance of the Study

The study is important because it aims to tackle the increasing cybersecurity requirements stemming from the Ethiopian government's Digital Ethiopia 2030 (DE2030) policy, as well as the establishment of the Mesob Digital Collaboration Ecosystem. With the increasing inter-connectivity of digital government systems, there is a growing need for a cyber-security framework that is sensitive to context to provide secure, resilient, and sustainable digital services.

2.8.1 The academic contribution of this study is that it enhances the body of knowledge in the field of cybersecurity with a focus on the context aware cybersecurity frameworks, specifically in the field of digital government security and interoperable systems. Furthermore, it serves as a reference for future studies in cybersecurity, e-government and Digital Transformation in the context of developing countries.

2.8.2 The practical significance of this study is that it can help enhance the security of digital systems in Ethiopia, particularly the Mesob ecosystem. It enhances the security of government platforms and mitigates risks like data breaches, ransomware attacks, unauthorized access, and service disruptions in the digital landscape.

2.8.3 Policy Significance: The study contributes to the creation of more robust cybersecurity policies, cybersecurity standards and coordination structures. It also helps build the national cyber security governance and take the institutional practices in line with the goals of the Digital Ethiopia 2030 strategy.

2.8.4 Technological Significance: This study has significance towards the technological security of digital systems by contributing towards secure interoperability, identity and access management, risk-based access control and continuous monitoring mechanisms. The enhancements boost the cyber resiliency of Ethiopia's digital infrastructure.

2.8.5 National Significance: The study helps to build trust in digital government services and ensure secure digital transformation with DE2030 at the national level. It is also seen as a way to mitigate the country's vulnerability to cyber threats and contribute to building a secure and resilient digital economy in Ethiopia.

2.9 Scope of the Study

This research focuses on creating a context-aware cybersecurity framework that will safeguard Ethiopia's Mesob Digital Collaboration Ecosystem, a crucial aspect of the country's Digital Ethiopia 2030

(DE2030) initiative. In particular, the goal is to ensure that when Ethiopia continues to progress in digital transformation, the security of government systems interconnections is adequately addressed.

Given the nature of digital government transformation, it is important to acknowledge that the scope of the study is intentionally restricted to the cybersecurity aspect of the digital government transformation, specifically in relation to the integration and inter-communication of government systems. Does not encompass the general areas of ICT development or non-security areas of digital transformation.

- **Focuses on cybersecurity in Ethiopia's digital government systems:** Identifies ways to safeguard government digital platforms, databases, and online services from cyber threats like hacking, data breaches, unauthorized access, and disruptions to systems.
- **Cybersecurity challenges of Mesob Digital Collaboration Ecosystem:** Discusses security issues arising in the Mesob platform such as secure data exchange between institutions, identity management, access control, and protection of sensitive citizen and government data.
- **Compliant with the Digital Ethiopia 2030 (DE2030) strategy:** Supports the long-term digital transformation vision of DE2030 in such a way that cybersecurity is used to ensure secure, trusted, and resilient digital government services.
- **Tackles problems related to system interoperability and digital integration:** Discusses security threats when various government systems are linked to each other, including data leakage between systems, insecure APIs, inconsistent security levels and vulnerabilities due to "integration.

3. Literature Review

Digital technologies are transforming how governments provide public services, handle citizen data and communicate with citizens. Worldwide, digitalization is a strategic priority for enhancing efficiency, transparency, accountability and accessibility of services. This transformation is a key priority in Ethiopia through the Digital Ethiopia 2030 (DE2030) strategy which focuses on the development of the digitally enabled economy and an integrated e-government system.

With the advent of digital platforms like e-government services, digital identity systems, cloud computing infrastructure and interoperable collaboration ecosystems in the government, cybersecurity is becoming more and more significant. The interdependent systems present complex security issues, such as data protection concerns, system vulnerabilities, and cyber threats to critical national information. Therefore, securing digital government infrastructure is a must to build trust, continuity of services and national security.

The aim of this literature review is to explore the current research and theory on digital transformation, cybersecurity issues, digital governance, cloud security, and new security methods like context-aware security. It also examines the cyber threat landscape in developing countries, focusing its examination on the cyber landscape in Ethiopia. In addition, it reveals research gaps, especially concerning the integration of cybersecurity frameworks for interdependent government systems like the Mesob Digital Collaboration Ecosystem.

3.1 Digital Transformation in Ethiopia

Digital transformation in Ethiopia is the country-wide transition from paper-based to fully integrated government services that leverage digital technology as a tool, in line with the Digital Ethiopia 2030 (DE2030) strategy. It involves the adoption of e-government platforms, digital identity systems, electronic payment systems and interoperable public service infrastructures. The overall goal is to enhance the efficiency, transparency and accessibility of service delivery to citizens and businesses. This rapid change, however, also brings about new cyber security demands, as increasingly sensitive government data is being stored and processed in digital environments.

3.2 Cybersecurity Challenges in Developing Countries

In the developing countries, there are several cybersecurity challenges that hinder secure digital transformation. These include lack of adequate ICT infrastructure, lack of skilled cyber security professionals, lack of cyber security awareness among users, and lack of strong institutional coordination. Furthermore, a lot of systems are dependent upon older or legacy technology that are extremely susceptible to attacks. The lack of resources also hinders the deployment of advanced security solutions like intrusion detection systems (IDS), security operation centers (SOC), and continuous monitoring frameworks.

3.3 Digital Governance and Collaboration Ecosystems

Digital governance ecosystems are ecosystems that bring together multiple government actors and put them in one digital service environment, provide data and services across platforms and platforms. The Mesob Digital Collaboration Ecosystem is a system designed to integrate ministries, agencies, and regional

offices, facilitating instant service delivery and data exchange. This helps with efficiency and coordination, but it adds complexity to the cybersecurity aspect. If one system becomes vulnerable, it can impact several institutions, which means a robust identity management system, access control and secure interoperability are crucial.

3.4 Cloud Computing and Shared Digital Infrastructure Security

Cloud computing is important to Ethiopia's digital transformation, providing scalable and cost-effective infrastructure. But shared Clouds bring up major security issues. They range from data privacy issues, multi-tenancy isolation issues, insecure APIs, misconfigured cloud services and unauthorized access to sensitive data. Because multiple government agencies may share the same infrastructure, it is vital to ensure that such systems are properly segmented, encrypted and conform to security standards to keep national digital assets secure.

3.5 Cyber Threat Landscape in Ethiopia

As Ethiopia is getting more digital, so is the cyber threat landscape. As Ethiopia has become more digital, so has the cyber threat landscape. Phishing attacks on government employees, ransomware attacks against institutional systems, distributed denial-of-service (DDoS) attacks on public services and website defacement are among the common threats. Weak access control policies continue to be an issue, too, because of insider threats. Furthermore, the areas that are considered critical, like banking, telecommunication, and government services, are gaining increasing popularity as the potential victim of any cybercriminal and politically motivated attacker.

3.6 Existing Cybersecurity Frameworks

There are several cyber security frameworks which are globally adopted and partially implemented in Ethiopia to guide security practices. These include ISO/IEC 27001 Information Security Management Systems, the NIST Cybersecurity Framework, as well as national ICT policies. These frameworks offer a framework for managing risks, responding to incidents and monitoring for continuous risks. There are however, gaps in implementation, as some institutions have limited technical capacity, lack of standardization within institutions, and limited enforcement.

3.7 Context-Aware Security Approaches

Context-aware security is a sophisticated security strategy that adapts security solutions according to context, including who is accessing the system, what type of device is being used, where it is accessed from, how it is being used and when it is being used. A system might for instance be able to be used normally from a trusted government office, but not when accessed from an unknown device or location. This helps to detect abnormal behaviour and minimise the risk of unauthorized entries in complex digital government environments.

3.8 Zero Trust Architecture

Zero Trust Architecture (ZTA) is a sophisticated cybersecurity approach that aims to protect contemporary digital environments by rejecting the notion of trust in the network. Zero Trust is fundamentally about “Never Trust, Always Verify” which is a different way of securing a perimeter than the traditional “Trust but verify.” While the traditional perimeter security mechanism is to trust and verify, Zero Trust is a “Never Trust, Always Verify” philosophy. This implies that all users, devices, applications and systems requesting access to digital resources must be constantly authenticated, authorized and verified, whether inside or outside the network environment.

Digital governance environments worldwide are vastly different today than they were in the past, particularly by the increasing use of cloud computing, digital identity systems, API-based interoperability, and integrated e-government platforms. The expansion of attack surface, connected infrastructures, and distributed service architectures have also raised cybersecurity concerns with these developments. Ethiopia's Mesob Digital Collaboration Ecosystem involves the sharing of data and co-ordination of services among different government institutions via interconnected digital platforms, which leaves sensitive government systems and national digital assets vulnerable to existing security models. Therefore, the Zero Trust Architecture is a more adaptive and resilient security architecture appropriate for securing the Digital Ethiopia 2030 (DE2030) transformation environment.

One of the core principles of Zero Trust Architecture is continuous identity verification. All access requests should be authenticated with robust authentication methods before access is allowed. These include technologies like Multi-Factor Authentication (MFA), Single Sign-On (SSO), biometric verification, and centralized Identity and Access Management (IAM) systems. Continuous authentication keeps users authenticated during active logins, which lowers the threats of credential theft, unauthorized access and identity compromise.

Least privilege access control is another key principle of Zero Trust. That is the principle that users, applications, and systems should be given the least necessary access to complete authorized functions. This helps to avoid unwarranted permissions and limit the chances of insider threats, privilege abuse, and unauthorized data exposure. In a connected

government environment like Mesob, least privilege policies are key because if one system is breached, a wide range of permissions could enable an attacker to traverse multiple institutions to move laterally.

Context-aware security is also given high priority in Zero Trust Architecture. Zero Trust does not depend on static security rules but rather dynamically analyzes contextual attributes, like user activity, location, device health, login history, time of access, and system threats. These contextual factors are constantly changing and are used to make decisions about access. For instance, if a user logs on to a system from a valid office workstation with a known device, they may be granted full access, but if a user logs on from a different device in an unknown location, they might be required to provide further forms of authentication prior to being granted access or be denied access altogether.

Another important element of Zero Trust Architecture is micro-segmentation. It includes segmenting networks and digital infrastructures into distinct pieces to stop lateral movement of cyber threats. Micro-segmentation is a technique that can be deployed to isolate the ministries, regional government systems, cloud infrastructure, databases, and critical digital services within Ethiopia's Mesob Digital Collaboration Ecosystem into distinct security segments. When one affected segment is compromised, it will not be able to spread through the rest of the ecosystem and reduce the impact of cyber incidents.

Continuous Monitoring & Real-Time Security Analytics is also part of Zero Trust Architecture. Security systems are continuously gathering and analyzing logs, API activities, user behaviors and network traffic to look for any anomalies and suspicious activities. Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), artificial intelligence threat detection, behavior analytics, etc., contribute to better proactively detecting cyber threats. Those capabilities enable quicker response to incidents and enhance the cyber resilience of interdependent digital government environments.

In Zero Trust environments, APIs and data exchange play a pivotal role in facilitating interoperability between institutions, making API security a critical element. Zero Trust based API security frameworks guarantee all API interactions are authenticated, encrypted, monitored and authorized by the security policies defined. API gateways, token-based authentication, and encrypted communication channels ensure that sensitive government information is not vulnerable to unauthorized access, manipulation, and interception.

Moreover, Zero Trust Architecture is quite supportive of the Zero Trust philosophy of “assume breach.” This means that a cyber attacker could be present in the network environment and that security systems should continuously be monitoring all activities for suspicious behavior. Continuous validation, automated policy enforcement and real-time monitoring make it harder for attackers to compromise systems within interdependent government systems to maintain a foothold or reach higher status.

Although the benefits are apparent, there are a number of challenges to implementing ZTA in the developing world, including in Ethiopia. These include the lack of the required IT infrastructure, lack of qualified cyber security personnel, outdated government systems incompatible with modern security solutions, lack of uniformity in cyber security policies and financial constraints to invest in high-tech security. Alongside, robust governance frameworks, inter-institutional coordination and national cyber security policy consensus are critical to the successful implementation of this, where proper policy integration is needed at all government institutions.

In conclusion, Zero Trust Architecture offers a modern, adaptive, and intelligent cybersecurity strategy to safeguard the dynamic and diverse cyber landscape of Ethiopia's digital government ecosystem. Micro-segmentation and context-aware security controls, along with the continuous verification of users, devices, and system activities, are just a few of the features that enhance cybersecurity resilience, increase trust in digital services, and enable the Mesob Digital Collaboration Ecosystem to operate securely through interoperability. The implementation of Zero Trust principles in the context of Ethiopia's Digital Ethiopia 2030 Strategy will play a critical role in ensuring the secure, reliable and sustainable realization of digital transformation in the country.

3.9 Research Gap Analysis

While strides have been made toward digital transformation and cybersecurity efforts, there are still substantial areas for research. There is little development of integrated cybersecurity frameworks that are designed for Ethiopia's digital government ecosystems. Studies in the field are generally aimed at generic cyber security issues instead of at specific issues like interoperability in platforms such as the Mesob Digital Collaboration Ecosystem. Also, there are no adaptive and contextual security models suited to government environments. This includes a lack of attention to a comprehensive and locally relevant cybersecurity framework that is in step with the aims of DE2030.

4. Research Methodology

The design of this study is guided by a mixed methods approach for examining the problems and needs for cybersecurity in the digital collaboration ecosystem in Ethiopia, specifically in the Mesob ecosystem. The approach is a mix of qualitative and quantitative methods, to provide a holistic view of the technical and institutional cyber security problems. The methodology is aimed at increasing the validity by using data triangulation and multiple data sources integration.

4.1 Research Design

The research design used is descriptive and exploratory. The descriptive design is employed to describe the current status of cyber security practices, risks and governance mechanisms in the digital government systems in Ethiopia in a systematic manner. The exploratory design is used to uncover the new challenges in the cybersecurity space, interoperability issues, and missing components in the current framework of the Mesob Digital Collaboration Ecosystem. This is a good choice for the analysis of complicated and changing digital environments.

4.2 Qualitative and Quantitative Research Approaches

The study is of mixed method in nature which is both qualitative and quantitative methods.

The qualitative approach is used to understand cybersecurity governance, institutional practice, the implementation of policies and experiences of cybersecurity experts. It provides in-depth insights into cybersecurity challenges and organizational behavior.

The quantitative approach is based on quantifiable data and measures of cybersecurity, including awareness ratings, risk exposures, readiness of systems, and policy adherence. It allows statistical assessment of cybersecurity situation.

Both approaches being integrated can help to provide a full analysis and can improve the credibility of the results because of methodological triangulation.

4.3 Data Collection Methods

Multiple complementary methods are used to gather data:

- **Semi-structured interviews:** Interviews conducted with cybersecurity experts, ICT managers, policymakers and system administrators to get detailed qualitative insights.
- **Structured questionnaires (surveys):** Sent to ICT professionals and government employees to collect the measurable quantitative data.
- **Document analysis:** Review of national cybersecurity strategies, Digital Ethiopia 2030 policy, institutional reports and international cybersecurity frameworks.

These techniques provide full coverage of data from a technical, organizational and policy standpoint.

4.4 Sampling Techniques

The study has used purposive sampling and stratified sampling.

- **Purposive sampling method:** Key informants with relevant expertise in cybersecurity and digital governance from the cybersecurity and policy sectors are identified and selected through purposive sampling.
- **Stratified sampling method** is employed to obtain representation of the various categories of institutions including ministries, agencies, regional offices and private ICT organizations.

This will allow for equal opportunities for technical and institutional actors to participate.

4.5 Data Analysis Methods

Both qualitative and quantitative methods of analysis are used.

- **Qualitative data analysis:** Thematic analysis is employed to discover patterns, themes, and cyber-security challenges from interview and document data.
- **Quantitative data analysis:** Statistical methods including frequencies, percent and descriptive analysis, are applied to analyze survey responses.

Both methods are integrated for better interpretation and to facilitate the triangulation of the data.

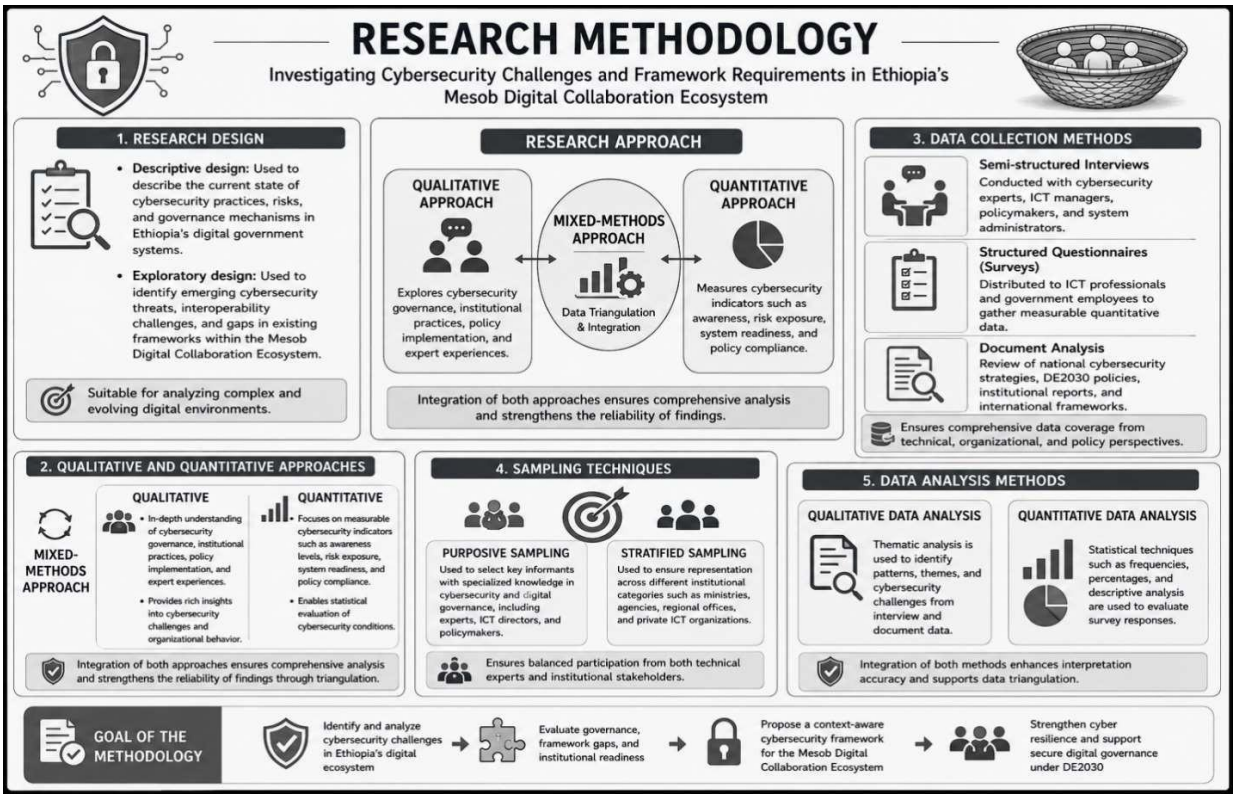

Figure 5. Mixed-methods research methodology

4.6 Ethical Considerations

This study is conducted based on the research ethical considerations so that it is carried out with integrity and ensuring the safety of research participants:

- **Informed consent:** Subjects are given information about the study before they enter.
- **Confidentiality:** All personal and institutional data is kept confidential and anonymized.
- **Security of data:** Collected data is kept securely with no unauthorized access.
- **Voluntary participation:** Any participation is voluntary and respondents may withdraw anytime.
- **Non-maleficence:** The study does not harm persons or institutions.
- **Academic integrity:** All sources cited properly, and all acknowledgments made.

5. Analysis of Ethiopia's Mesob Digital Collaboration Ecosystem

The Mesob Digital Collaboration Ecosystem is a new national Digital Integration framework that brings together government institutions, aligns public service delivery and facilitates secure data sharing among the public sector in Ethiopia. It is a major contributor to the country's Digital Ethiopia 2030 (DE2030) policy and framework, which has committed to a move from a fragmented administrative system to a single, data-driven approach to digital governance. The scientific and systems approach to the understanding of an ecosystem is one that can be viewed as an environment that is socio-technical, with continuous interactions between its technology, institutions, policies and users. It brings efficiency and coordination, but it also poses a great deal of cyber security risk because of its greater interconnectivity and data dependence.

5.1 Overview of Ethiopia's Digital Ecosystem

Digital Ethiopia is a coordinated, developing and structured environment, that brings together digital infrastructure, government platforms and institutional services into a coherent national system. It aims to facilitate digital governance, optimize service delivery, and increase transparency through tech-driven processes. The ecosystem is still evolving, and there is a gradual integration of the old with the new systems.

- The ecosystem is in line with the Digital Ethiopia 2030 policy, which is underpinned by digital transformation of government and economic modernization. The ecosystem is directed towards digital government transformation and economic modernization which is part of the Digital Ethiopia 2030 policy.
- It incorporates several layers such as infrastructure, platforms, applications and governance frameworks.

- Its vision is to move away from a silo mentality in government systems towards interoperable and shared digital services.
- It encompasses centralized and distributed digital systems for both federal and regional institutions.
- However, it still has a long way to go in maturity issues such as standardization, interoperability and cyber security readiness.
- It is a step towards moving from a manual governance to a digital government driven by data.
- It relies more on common facilities like cloud systems, data centers, and country networks, and is increasingly so.

5.2 Government Digital Platforms and Services

Government digital platforms are the part of Ethiopia's digital ecosystem where government services are provided to citizens and businesses electronically. The purpose of these systems is to make government services more efficient, streamline bureaucracy and make them more accessible.

- Civil registration and national digital identity systems for citizen verification and authentication
- The legal framework and provisions for electronic filing and payment of taxes and revenue collection systems
- Passport, immigration and travel document management systems
- Information systems for public health monitoring and patient information management
- Education management systems that facilitate student records, examinations and institutional administration.
- Digital financial systems, which will facilitate financial payments and e-service transactions for government services
- Platforms for business registration and compliance management (licensing and regulatory)
- There is still significant interoperability lack between platforms with many systems running independently.
- Security implementation is found to be different between institutions and hence, different institutions have different levels of security.
- Data exchange mechanisms are still in their infancy and frequently require manual and semi-automated integration.

5.3 Inter-Institutional Digital Collaboration

Inter-institutional collaboration within the Mesob ecosystem is the digital exchange and interaction between ministries, agencies and bodies of regional government. For the delivery of integrated services and effective coordination of service provision, this collaboration is vital.

- Allows for government institutions to share data in real-time or near real-time.
- Allows access to and analysis of integrated data for joint decision making; and
- Minimizes duplication of services and administration between institutions
- Leverages APIs, middleware, and common integration platforms extensively
- Needs to have uniform ID/Mgmt of identities across institutions
- Faces challenges because of non-uniform technical standards between government organizations.
- Develops a high interdependency culture in which failure of one part of a system can lead to failure of another.
- Raises cybersecurity hazards because of the added attack surfaces in systems that are connected together.
- Needs robust governance and framework to assure a secure interoperability.
- Needs centralized monitoring and coordination mechanisms for effective security control.

5.4 Digital Infrastructure and Connectivity

The digital infrastructure for Ethiopia's Mesob system consists of various interrelated technologies that facilitate the transmission of communication, processing of data and provision of services among institutions. This is the foundation of the overall digital transformation effort.

- National telecom infrastructure that delivers mobile and fixed services
- Government data centers with critical national information systems and applications
- Scalable and shared environment for government services in the cloud (Services on the cloud)
- Internet backbone infrastructure for national and international connectivity.
- Institutional IT systems (servers, endpoints, internal networks, etc.)
- Growth of hybrid infrastructure models (cloud + on-premise)
- Inconsistency in the distribution of infrastructure in urban and rural areas that affects services
- Some critical systems are not sufficiently redundant and do not have disaster recovery capability.
- Dependency on centralized infrastructure points increasing risk of single points of failure
- Increasing demand for network segmentation and resilient architecture design for security.

5.5 Major Cybersecurity Risks and Vulnerabilities

What they are, how to identify them, and how to manage them. With its interdependent design, shared resources, and growing digital reliance, the Mesob

Digital Collaboration Ecosystem is vulnerable to a variety of cybersecurity threats. These risks have a negative impact on the security of government information and services with regard to confidentiality, integrity and availability.

- Attacks on government employees and system users using phishing and social engineering techniques.
- Ransomware attacks to encrypt critical government systems and interrupt service delivery
- Distributed Denial of Service (DDoS) attacks on public facing digital services.
- Insider threats due to misuse of privileged access or inadequate monitoring systems
- Security issues with API used in system integration and data exchange mechanism.
- Risk of data leakage during communication and sharing of data between different institutions.
- Lack of good authentication and access control provision in some legacy systems
- Misconfiguration of cloud services allowing unauthorized access to the cloud resources or inappropriate disclosure of data.
- The absence of ongoing monitoring and identification of threats in some institutions.
- Risks, because of system interoperability, increase due to larger attack surfaces.
- Lack of cybersecurity knowledge among end users resulting in human factor weaknesses

5.6 Regulatory and Governance Challenges

The governance of cybersecurity in the Ethiopian digital ecosystem is still evolving and is constrained by various structural, operational and regulatory challenges. The problems faced involve the uniformity of implementing the cyber security controls among institutions.

- No fully integrated and coordinated national cybersecurity governance and coordination framework.
- Incomplete institutional roles with overlapping and/or unclear mandates
- Inadequate implementation of cyber security policies, standards, and compliance measures
- Limited interoperability security standards with regards to system integration, data exchange
- Insufficient data protection and privacy regulation enforcement mechanisms
- Inconsistent cybersecurity maturity levels across different government institutions
- Lack of cybersecurity professionals in the public sector
- A lack of investment in cutting-edge cybersecurity technologies and monitoring systems
- Lack of coordination of incident response between institutions in cyber events.
- Lack of common audit and compliance standards for digital government systems
- Relying on third parties who don't have effective security protocols in place.
- The need for greater alignment of the goals of the Digital Ethiopia 2030 with cyber security enforcement mechanisms

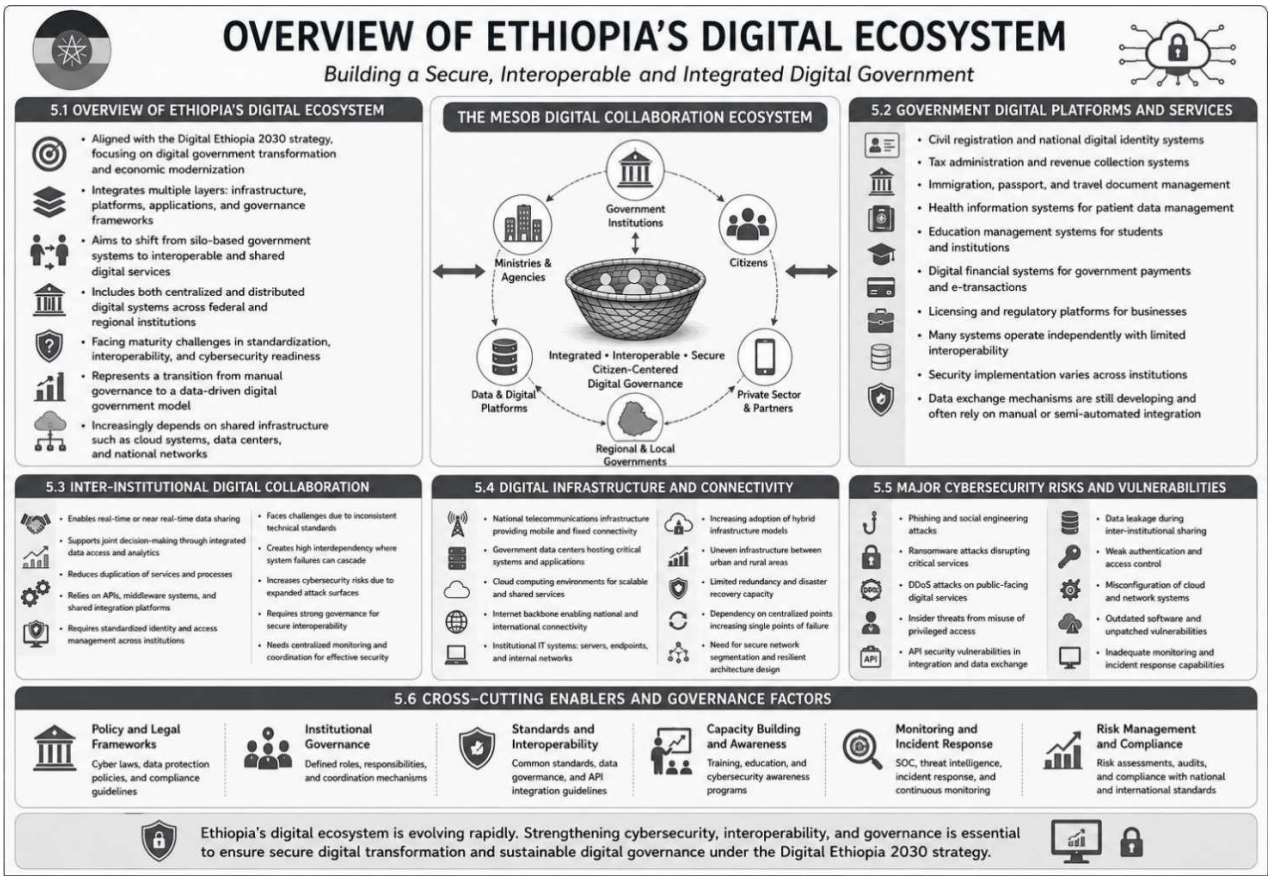

Figure 6, Overview of Ethiopia's Digital Ecosystem

6. Proposed Context-Aware Cybersecurity Framework

The proposed Cybersecurity Framework for the Context-Aware is a scientifically designed security model developed to secure the highly interconnected and interdependent government institutions, shared digital infrastructures and interoperable service platforms of Ethiopia's Mesob Digital Collaboration Ecosystem. The framework presents a flexible and intelligent cybersecurity strategy, addressing the previous challenges, including integration risks, security control inconsistencies, a lack of monitoring capabilities, and the rising cyber threats. It makes sure that security actions are not fixed, but rather flexible and adaptable according to context, including who the user is, how the device is being used, where it's being used and what the risk to the system is. The framework is aligned to the Digital Ethiopia 2030 strategy and it is meant to enhance the national cyber-resilience, facilitate information exchange and to promote trustworthy digital governance.

6.1 Framework Overview

The framework overview outlines the general features and goal of the suggested cybersecurity model. It combines technical, organizational and governance elements into a single system to secure interconnected government environments. The framework provides common security principles for all digital government systems and a level of flexibility for the different needs of institutions. It also establishes context-awareness as a fundamental concept, where security controls automatically respond to risk situations and context. With this, the Mesob ecosystem will continue to be safe even though it grows and adds more services.

- Ensures uniformity of the entire security system of all government systems that are interconnected, thus eliminating the diversity and security gaps between platforms.
- Promotes the security of interoperable digital platforms, safeguarding data sharing pathways, APIs, and platform integration between ministries and agencies.
- Comparands preventative, detective and responsive controls, all working as one within a unified framework, including the firewalls, intrusion detection, monitoring and incident response.

- Implements context-awareness: dynamically changes decisions on security based on users, their location, their device trust level, and their access patterns.
- Facilitates secure data transfer, including encryption and management of data communications between institutions.
- Engages in national digital transformation agendas and contributes to the vision of Digital Ethiopia 2030 on the theme of digital governance that is security and efficient.
- Improves resilience to cyber threats by offering a multi-layered defence against attacks on interconnected systems.

6.2 Context-Aware Security Architecture

The context-aware security architecture is a multi-layered cybersecurity framework that will offer adaptive and intelligent security protection to the Ethiopia's Mesob Digital Collaboration Ecosystem (DCE). This architecture continuously assesses real-time context—user activity, device state, location and system activity—before granting access or taking action, unlike traditional security systems that use fixed rules. This means that each interaction on the digital landscape is dynamically evaluated for risk, allowing the system to be more resistant to current cyber threats.

Every layer serves a specific purpose in enhancing the overall security;

- The **identity layer** is a part of the system that validates the authenticity of users using secure digital identity systems. It helps to ensure only authorized and valid users have access to government systems, thus minimizing the threat of impersonation, credential theft, and unauthorized access.
- The **context layer** processes real time environmental and behavioral information (where user logged in, device used, when they accessed it, how they used it). These context clues are used to identify if a requested access is "normal" or a “potential risk”.
- The **policy layer** implements adaptive security rules according to the result of the risk assessment. Rather than setting permission levels, it adaptively varies permissions, which means that high-risk activities might be required to raise the level of authentication, or it may be denied completely.
- The **application layer** defends government digital services by directly embedding security controls within e-government applications. This will provide security at the service level, as well as at the network edge.
- The **data layer** guarantees the security, integrity and controlled data exchange between institutions. It controls data storage, access and movement in the ecosystem to stop data leakage or unauthorized modification.
- The **infrastructure layer** ensures the security of the technical environment, such as cloud resources, networks, and data centers. It is to protect systems and services that are vital for all digital services.
- The **analytics layer** employs sophisticated analysis methods like machine learning and behavioral analysis to identify real-time patterns, anomalies and potential cyber-attacks.
- The **zero-trust model** means that all users, devices, and systems should be treated as non-trusted, even within the network. All accesses should be continually checked, even if they are from a different entity or were already authenticated.
- All activities throughout the ecosystem are recorded in the central logging system, providing accountability, transparency and traceability. After security incidents, these logs are important for auditing, monitoring and forensic analysis.

6.3 Adaptive Access Control Mechanisms

Adaptive access control is a real-time, context-situated cybersecurity mechanism that manages user permissions which dynamically changes as per the real time security risk assessment. Traditional access control models are based on roles or static permissions, while adaptive access control constantly assesses the security dynamics and adjusts access as necessary. Given the context of the Mesob Digital Collaboration Ecosystem in Ethiopia, where various government systems are interdependent, and vulnerable to new cyber threats, this is very appropriate. It combines all of these elements to make access decisions secure and context-sensitive.

All of the adaptive access control elements help to increase the overall security of the system:

- **Role-Based Access Control (RBAC)** allows for the orderly and hierarchical distribution of access to a data center in government institutions, based on organizational roles, and reduces the granting of unnecessary access.
- **Attribute-Based Access Control (ABAC)** takes a step further by considering other attribute factors like user's department, job function, clearance level and operational requirements, allowing more fine-grained and context specific access decisions.
- **Risk-Based Authentication** RBA dynamically adjusts the level of authentication depending on

the risk of the login attempt; thus, higher risk levels result in higher levels of authentication.

- **Multi-Factor Authentication (MFA)** By demanding more than one independent credential like a password, OTP, or biometric factor, Multi-Factor Authentication (MFA) makes it harder to access the data, further minimizing the chance of unauthorized access.
- **Device trust assessment** is the process of analyzing and assessing the security posture and compliance of the device that is being utilized, ensuring that only those that are trusted and secure can gain access to sensitive systems.
- **Location and time-based restrictions:** By restricting access attempts from unusual geographic locations or abnormal times, location and time-based restrictions help to detect and block suspicious login behaviors.
- **Continuous session monitoring:** The ability to monitor sessions continuously keeps a close watch on user activity during active sessions and identifies any irregular usage patterns at real time, which enables the early detection of any inner threats or compromised account usage.
- **Automatic session termination** automatically terminates users' sessions when suspicious or high-risk activity is detected, helping to limit the potential damage caused by compromised credentials or unauthorized actions.
- **Integration with national digital identity systems** Incorporating national digital identity systems helps that they are verified and centralized, leading to better trust and lowering identity fraud dangers.
- **Policy-driven authorization** provides the system with the ability to make access control decisions based on dynamic and adaptive security policies instead of static policies, and to react intelligently to the changing threat conditions.

In summary, adaptive access control offers a flexible, intelligent, and risk-aware security approach that has a significant impact on the level of protection in complex and interconnected digital government environments.

6.4 Threat Intelligence and Risk Management

Threat intelligence and risk management is a proactive capability within cyber security that can improve the capability of government systems to anticipate, detect, analyze and respond to cyber threats prior to serious damage. Within Ethiopia's Mesob Digital Collaboration Ecosystem, in which several institutions are connected, this component is vital in sustaining situational awareness, and enabling a more proactive approach to security decisions based upon real-time intelligence and predictive analytics instead of incident response. It allows transitioning from the traditional security paradigm (defensive) to the intelligence paradigm (Cyber security).

This component makes coordinated and systematic contributions towards a robust national cyber defense:

- A central threat intelligence platform allows the integration, aggregation and dissemination of threat intelligence information throughout all government entities, thus allowing for joint defense and diminishing individual security responses.
- The continuous gathering of Indicators of Compromise (IOCs) helps identify malicious activity at an early stage, by recognizing known attack signatures and suspicious activity, as well as emerging patterns of threats.
- Real-time risk scoring: It means judging the risk level for current activities and giving systems, users and transactions dynamic risk scores so that security teams can prioritize their response.
- Predictive analytics leverages historical attack information, patterns, and trends to anticipate future attacks and take security measures in advance of the attack.
- Cross-institutional incident correlation allows security events on different government systems to be correlated to identify a coordinated or distributed attack on several institutions at once.
- Internal and external intelligence sources are integrated, adding to situational awareness by integrating organizational logs, global threat intelligence feeds and security databases.
- Automated threat classification prioritizes cyber threats by severity, impact and urgency, meaning critical threats are given immediate attention.
- The proactive identification of vulnerabilities continuously scans systems to identify vulnerabilities, misconfigurations, and other weaknesses that could be exploited by attackers.
- Compliance with national cybersecurity strategies and policies means all the threat intelligence activities meet government policies, standards and regulations.
- The system helps make informed decisions by offering security analysts and policymakers actionable, timely, and context-relevant intelligence to enable effective cybersecurity governance.

Overall, this part enables cybersecurity processes to evolve into a predictive and intelligence-led defense strategy, enhancing the resilience of interconnected digital government environments to new cyber threats.

6.5 Continuous Monitoring and Incident Response

Continuous monitoring and incident response is an essential cybersecurity skill that facilitates real-time visibility, detection and timely response to security incidents in Ethiopia's Mesob Digital Collaboration Ecosystem. Monitoring is a critical process in maintaining the integrity, availability and trust of the system, especially in today's highly interconnected government environment where multiple institutions share data and services. It allows companies to shift from a reactive incident-handling system to a coordinated, real-time, automated security response system designed to minimize the damage and time needed to recover.

All of the pieces are crucial to the successful execution of a cybersecurity operation:

- The **Security Operations Center (SOC)** is the centralized point from which organizations monitor and coordinate security operations to detect and manage security events across all government institutions in a coordinated and unified way.
- **Continuous log** collection provides detailed activity information for applications, networks, servers and infrastructure systems, ensuring complete visibility and forensic analysis of system behavior.
- **Anomaly detection:** This uses real-time analytics to detect abnormal behaviors of the users or systems that may be indicative of cyberattacks, insider threats, or compromised accounts.
- **Suspicious activities** are automatically alerted to security teams, allowing for quick investigation and response.
- **Structured Incident Response Process:** A set of standardized procedures for incident detection, containment, recovery, and learning to handle all security incidents in the same way.
- **Forensic analysis** capabilities enable detailed investigation of cyber incidents to gain a greater understanding of the origin, impact, and attack methods in order to bolster future defenses.
- **Automated containment** actions detect threats to affected systems or accounts and isolate them, thereby stopping attacks from propagating across systems that are interconnected.
- **Inter-agency coordination** mechanisms facilitate coordination among various government agencies in the event of a security incident, thus providing a common national response.
- **Business continuity** integration enables business continuity for vital government services during cyber events or system failure.
- **Continuous system** monitoring continuously evaluates the health, performance and security of systems to detect vulnerabilities and operational concerns as early as possible.

Overall, continuous monitoring and incident response creates a real-time defense security environment that improves resilience, response time and stability of Ethiopia's digital government ecosystem.

6.6 Data Protection and Privacy Controls

Data Protection and Privacy Controls – 6.6

An important facet of the proposed Context-Aware Cybersecurity Framework involves data protection and privacy controls, which would help safeguard government and citizen information across its entire lifespan from creation to storage, processing and sharing, and eventual deletion. For Ethiopia's Mesob Digital Collaboration Ecosystem, where data is often shared between various entities, these controls are critical to ensure confidentiality, integrity, and trust in digital government systems. The goal is to avoid unauthorized access, minimise data exposure threats and comply with national and international data protection regulations.

All the components play a structured and systematic role in bolstering privacy and data security:

- Data is stored or transmitted securely using end-to-end encryption, meaning that if it is retrieved by someone else it will not be readable or modifiable without the correct encryption key.
- Data classification: Classifying data by level of sensitivity, including public, internal, confidential and restricted, to provide an appropriate level of security to the data depending on its sensitivity and importance.
- Data sharing mechanisms are secure and only authorized government institutions have access to or access to exchange data, thus preventing unauthorized exposure of data cross systems.
- By tokenizing and anonymizing data, sensitive information is replaced by secure identifiers or masked values, minimizing the risk of personal or critical information being exposed during processing or analysis.
- Access logging systems are used to keep track of all data access and modification activities, ensuring accountability, traceability, and audit capabilities for security monitoring and compliance verification.
- The principles of data minimization strive to minimize unnecessary exposure risks and attack surfaces by limiting the amount of data collected and processed.
- All data transfers between connected systems are authenticated, authorized and encrypted with the use of secure API gateways that control and monitor all communication between institutions.

- Compliance with data protection regulations helps to ensure that all data handling practices are in accordance with data protection laws, regulations and policies at the national and institutional level.
- Backup and Recovery mechanisms ensure that data is not lost, corrupted, or compromised by cyberattacks by preserving copies of the data for use in the event of a failure or incident.
- Data leakage prevention mechanisms (DLP) are used to continuously monitor the flow of data and prevent unauthorized transmission of sensitive data outside of approved systems or channels.

In sum, these controls create a broad privacy and data protection regime to protect sensitive data, enable better trust in digital government services, and facilitate trusted interoperability in Ethiopia's digital system.

6.7 Governance, Compliance, and Policy Integration

The proposed framework for Cybersecurity in the context is the governance and compliance framework. Technical controls are deployable on the operational level, while governance is the means to ensure the consistent enforcement of cybersecurity via policies, regulations, organizational structures, and inter-agency coordination. Governance and compliance play a crucial role in the sustainability, accountability, and harmonization of security practice across the various interconnected government institutions within the framework of the Mesob Digital Collaboration Ecosystem in Ethiopia. This layer ensures that cyber security is not disorganized, fragmented or institution-specific but a coordinated security system in line with Digital Ethiopia 2030.

In an organized way, each component helps to build the maturity of the institutional cybersecurity:

- A single cybersecurity governance mechanism provides a coherent cybersecurity coordination and control framework throughout the government, preventing cybersecurity governance fragmentation and enhancing cybersecurity control at the national level.
- Strategic, operational and technical accountability for cybersecurity management is defined by clearly defined roles and responsibilities, ensuring that all institutions are aware of the cybersecurity responsibilities they have.
- Alignment with Digital Ethiopia 2030 (DE2030) guarantees alignment of cybersecurity activities with national digitalization vision and long-term development plans.
- The standardization of cyber security policies ensures that all Government institutions implement the same security procedures which minimizes the variability in the implementation of cyber security and decreases security gaps.
- Availability of compliance to international standards like ISO and NIST will improve global compatibility, maturity of information security and adoption of best practices in the management of information security.
- Regular cybersecurity audits continuously assess the effectiveness of the systems, uncover vulnerabilities, and ensure that the systems comply with the security policies and standards.
- Legislation and regulation facilitate enforcement of cyber security legislation, data protection obligations and accountability for incidents within institutions.
- There are inter-agency coordination mechanisms that foster inter-agency collaboration during security operations, thereby providing a coordinated response for cyber incidents.
- Policy-based system configuration provides a way to automatically apply security controls using system policies, thereby minimizing human error and the consistency of security controls.
- An ongoing policy improvement process allows for a cybersecurity policy to adapt to new threats, technology, and risk environments.

In sum, governance and compliance provide a system of cybersecurity management that is structured, enforceable, and adaptive for long-term cybersecurity sustainability for the digital government system in Ethiopia and establishes the framework of institutional cybersecurity accountability and consistent cybersecurity implementation.

6.8 Framework Implementation Model

The implementation model is the systematic and phased deployment model of the proposed Context-Aware Cybersecurity Framework in the digital ecosystem of Ethiopia. It promotes gradual, coordinated and institutionally prepared and capable adoption, and ensures that it is in line with governance, institutional readiness and technical capacity. This step-by-step approach is crucial for the Mesob Digital Collaboration Ecosystem, as it enables the government institutions to gradually incorporate cutting-edge cybersecurity solutions without significantly disrupting the current services, while maintaining sustainability and operational stability.

Each phase helps to establish a mature and resilient cyber environment:

- **Phase 1:** System assessment and cybersecurity maturity evaluation is the first phase, which is where the existing government systems are analyzed to uncover security gaps, vulnerabilities,

and readiness levels, which serve as the foundation for the implementation of the framework.

- **Phase 2:** Governance and policy alignment is about setting up cybersecurity governance and aligning policies across institutions for consistent and coordinated security management.
- **In Phase 3:** The core security infrastructure deployment adds key elements like Security Operations Centers (SOC), monitoring systems, identity management systems, and fundamental cybersecurity tools.
- **Phase 4:** Integration of context-aware security mechanisms allows for adaptive access control and real-time risk evaluation systems, providing dynamic and intelligent security decision-making.
- **Phase 5:** Deployment of threat intelligence sharing platform and secure, real-time sharing of cyber security intelligence among government institutes to enhance collective defense and situational awareness.
- **Phase 6:** Capacity building and human resource development is about training, awareness creation and skill development to bridge the cybersecurity workforce gaps and build institutional readiness.
- **Phase 7:** Full-scale deployment & institutional integration: The framework is put in place in all government digital systems, leading to a cybersecurity standardization throughout the country.
- The Cybersecurity audit and compliance mechanisms continuously evaluate systems, processes and controls against agreed policies, standards (including ISO and NIST) and national regulations. Regular audits enable the discovery of gaps, accountability and compliance with stated cybersecurity requirements for all institutions. Compliance monitoring ensures uniformity of security practices, measurability and legal enforceability throughout the ecosystem.
- Evaluation and improvement allow for an ongoing review of system performance, making it possible to add updates, optimize and adapt to new cyber threats.
- Integration with national digital identity systems enhances authentication processes and fosters better interoperability between government platforms, providing trusted and consistent identity verification.
- Long-term sustainability of ownership and policies will ensure cybersecurity practices are part of government operations, backed by robust policies, leadership buy-in and regular governance processes.

In general, the implementation model provides a structured, scalable and sustainable cyber security transformation process, which will benefit the digital government ecosystem of the country, enhance the resilience of Ethiopia and increase interoperability security and coherence with the Digital Ethiopia 2030 strategy.

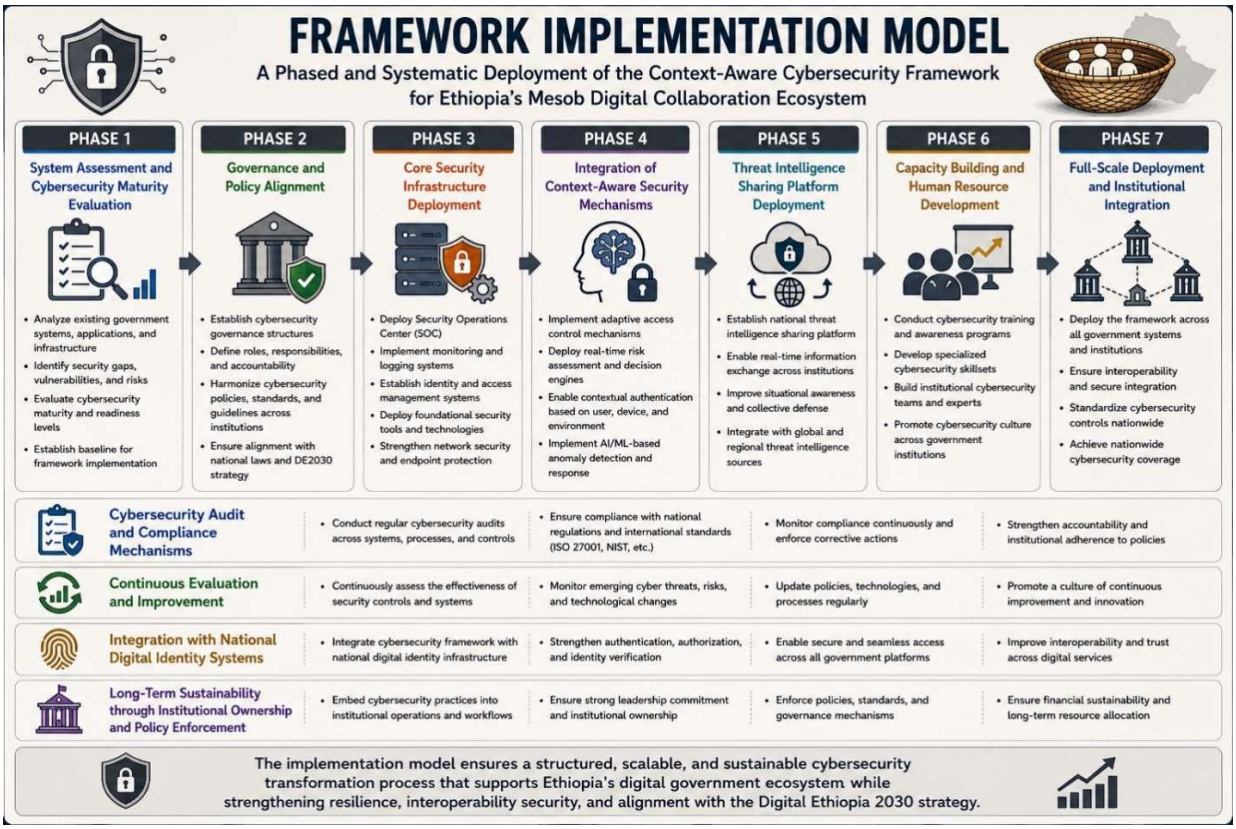

Figure 7, cyber security Framework Implementation Model

7. Results and Discussion

Based on the findings of this study, the proposed cybersecurity framework is proved to be effective in enhancing the overall governance coordination and system visibility of the digital ecosystem in Ethiopia, as well as the institutional integration. It offers a single security strategy that helps to improve the interoperability and ability to implement this strategy at a national level by meeting the goals of Digital Ethiopia 2030, and at scale.

Security effectiveness analysis shows the effectiveness of the framework, which enhances threat detection, prevention, and response capabilities by combining SOC, IAM, encryption, and continuous monitoring. This leads to increased security of digital systems and increased Confidentiality, Integrity, and Availability (CIA).

The framework also plays a part in Digital Ethiopia 2030 by fostering trust in digital services, enhancing data security and facilitating safe e-governance. Yet issues like a lack of skills, high implementation costs, poor coordination and legacy system integration pose real obstacles.

In comparison, international standards such as NIST, ISO 27001, COBIT offer very good standards but lack a complete contextual adaptation. The proposed framework is more appropriate for Ethiopia because it addresses the need for digital transformation in Ethiopia.

- The Digital Ethiopia 2030 (DE2030) Strategy and the Mesob Digital Collaboration Ecosystem are fostering the digital transformation by introducing interoperability in government systems, digital identity platforms, cloud computing and integrated public services in Ethiopia.
- Significant cybersecurity gaps remain, including with regard to security capabilities of interoperability technologies, lack of a strong governance framework, inconsistent security controls and implementation of advanced technologies for cybersecurity.
- Specifically, most current cybersecurity frameworks are widely applicable international models which do not comprehensively tackle Ethiopia's technological, institutional, infrastructural and governance issues and concerns.
- Ethiopia's digital governance is characterised by low adoption of advanced cybersecurity practices, including Zero Trust Architecture, context-aware security, adaptive access control, artificial intelligence for threat detection, and continuous monitoring.

- These challenges emphasize the pressing need for a comprehensive, context-aware, adaptive and locally relevant cybersecurity framework that would help enhance national cyber resilience, cyber interoperability and sustainable digital transformation in Ethiopia with the objectives of DE2030.

7.1 Framework Evaluation

The proposed cybersecurity framework is evaluated and shown to be complete and well-structured security model for Ethiopia's digital ecosystem. Results show that the framework was able to incorporate governance, technical security measures and operational monitoring into one integrated framework. This integration has benefits for effective coordination between institutions, decreased fragmentation of current cybersecurity processes, and increased overall system visibility.

In terms of the scientific results of the evaluation, it is demonstrated that the framework has a positive impact on the efficiency and alignment of governance in the digital government environment. It provides a standardized way to enforce security in multiple institutions and facilitates scaling up for a national level implementation.

- The architecture enables enhanced centralized security monitoring and visibility into systems.
- It enhances interoperability between heterogeneous government platforms
- It provides a consistent application of cybersecurity policy throughout institutions
- It enhances coordination among technical and administrative stakeholders.
- It facilitates scalable deployment from a pilot system to national infrastructure.
- It provides greater decision-making capability by integrating security information.

7.2 Security Effectiveness Analysis

Overall, the proposed framework promises to be a strong improvement in the security of digital systems from various cyber threats, such as unauthorized access, malware attacks, data breaches, phishing attacks, and insider threats. The findings illustrate enhanced detection, prevention and response capabilities.

In a scientific context, the combination of SOC, IAM, encryption solutions, and continuous monitoring systems can provide a layered security approach, making the systems more resilient.

- Real-time threat detection capability is greatly enhanced with SOC monitoring.
- Automated alerts and escalation powers down incident response time.
- Access to unauthorized resources is restricted by enforcing IAM.IAM is enforced to minimise access to unauthorized resources.
- Data encryption is improved for data in transit and at rest
- Security assessments are performed on a continuous basis reducing exposure of system vulnerability.
- Resilience of the whole system is enhanced with layered defense system architecture.
- Security visibility and control is improved with centralized monitoring systems.

The findings show, from a scientific point of view, the shift from reactive security model to proactive and adaptive cybersecurity model which enhances the Confidentiality, Integrity and Availability (CIA) of digital systems.

7.3 Benefits for Digital Ethiopia 2030

It is evident from the results that the proposed cyber security framework contributes greatly to the goals of the Digital Ethiopia 2030 strategy. The cybersecurity framework is built into the backbone of digital transformation, providing the foundations of secure, reliable and sustainable digital government services.

- It increases trust and confidence in digital government services
- It enhances the reliability and availabilities of the national digital platforms.
- Enhances the security of citizen and institutional information
- It allows for secure data sharing and interoperability among institutions
- It supports scalable and resilient e-governance systems
- It lowers the number of risks involved in a large-scale digital transformation.
- It increases the efficiency of delivering digital services in different industries

From a scientific perspective, the research shows that cybersecurity plays a pivotal role in digital transformation, impacting its adoption, usability, and institutional trust in digital services.

7.4 Challenges of Framework Implementation

However, there are challenges in implementing the proposed framework that could impact implementation on a full-scale basis. These are primarily institutional, financial and infrastructural challenges.

- Lack of cybersecurity skills and technical expertise.
- One of the challenges is that the cost of implementing SOC, SIEM and advanced monitoring systems is high.
- Lack of coordination and communication between government institutions.

- All of these are highly generalizable.
- Challenge of connecting legacy systems with new security infrastructure
- There is a lack of understanding about cybersecurity among users and the administrators.
- The most significant gap is the unevenness in infrastructure development of ICT across the regions and institutions.

In terms of scientific findings, non-technical factors are the major constraints, meaning that institutional reform, capacity building, and a gradual deployment approach are required to achieve successful implementation.

7.5 Comparative Analysis with Existing Frameworks

The comparative analysis reveals that despite the provision of solid foundation principles, the current cybersecurity frameworks like NIST Cybersecurity Framework, ISO/IEC 27001 and COBIT are not fully optimized to the national context of a digital transformation in Ethiopia.

- The NIST Cybersecurity Framework has a strong emphasis on risk management, and is weak on national system integration.
- ISO/IEC 27001: Tight compliance emphasis with less flexibility in the implementation of operational cybersecurity
- The COBIT model is a good governance model, however it does not have actual real-time cybersecurity capabilities.
- In addition, there are global frameworks, which are geared towards generic enterprise applications and not the national scale of an ecosystem.

By contrast, the proposed model illustrates greater contextual appropriateness and adaptability to operations.

- It integrates governance, technical controls, and interoperability into a single framework
- It facilitates the co-ordination of activities at the national level among various government systems.
- This allows real-time monitoring and centralized cybersecurity management.
- It is aligned with Digital Ethiopia 2030 strategic objectives
- It is specifically developed for the needs of a digital transformation in the public sector.

Overall, the Cybersecurity Maturity Level of Ethiopia: Current Status and 5-Year Projection is developing to intermediate. In terms of tangible results the country has achieved significant strides through the Digital Ethiopia 2030 Strategy, the Mesob Digital Collaboration Ecosystem, the scaling up of digital government services, the Fayda Digital ID initiative, the development of SOC capabilities and the cybersecurity governance under the INSA. Despite this, there remains a lack of maturity in cybersecurity among institutions.

Ethiopia has several challenges including poor cybersecurity governance, lack of interoperability security, lack of cybersecurity professionals, inconsistent implementation of security controls, low public cybersecurity awareness, lack of advanced threat detection and emerging adoption of Zero Trust. Ethiopia is set to become much more mature in the field of cybersecurity in the next half decade based on the proposed Context-Aware Cybersecurity Framework. Built into the framework: Zero Trust Architecture, SOC/SIEM, Identity and Access Management (IAM), Adaptive access control, AI-based threat detection, Encryption, Threat intelligence sharing, Continuous monitoring. These mechanisms should enhance cyber resilience, cyber interoperability security, threat detection, cyber governance coordination, cyber digital trust, cyber cloud security, cyber incident response, and monitoring capability.

As a result, after the expected implementation of the proposed framework, Ethiopia's cybersecurity ecosystem will move from the fragmented, reactive, to a proactive, adaptive, integrated, scalable, and resilient national cybersecurity ecosystem that aligns with the goals of the Digital Ethiopia 2030 Strategy and the Mesob Digital Collaboration Ecosystem.

The discussions on comparative analysis and the cybersecurity framework are conceptually linked with international digital transformation and cybersecurity standards, governance models, and scientific reports from various organizations including ITU, World Bank GovTech, GSMA Mobile Economy, United Nations E-Government Survey, NIST, ISO/IEC 27001, COBIT, INSA, and Digital Ethiopia 2030 Strategy. The cybersecurity maturity of Ethiopia's digital ecosystem is projected to greatly increase over the next five years, including in the cyber resilience, interoperability security, threat detection capability, governance coordination, digital trust, and continuous monitoring effectiveness domains based on current assessment and the planned implementation of the Context-Aware Cybersecurity Framework. The graphical analysis illustrates the shift from disjointed and reactive approaches to cybersecurity to more proactive, adaptive, and integrated national cybersecurity landscape that will serve the goals of Digital Ethiopia 2030.

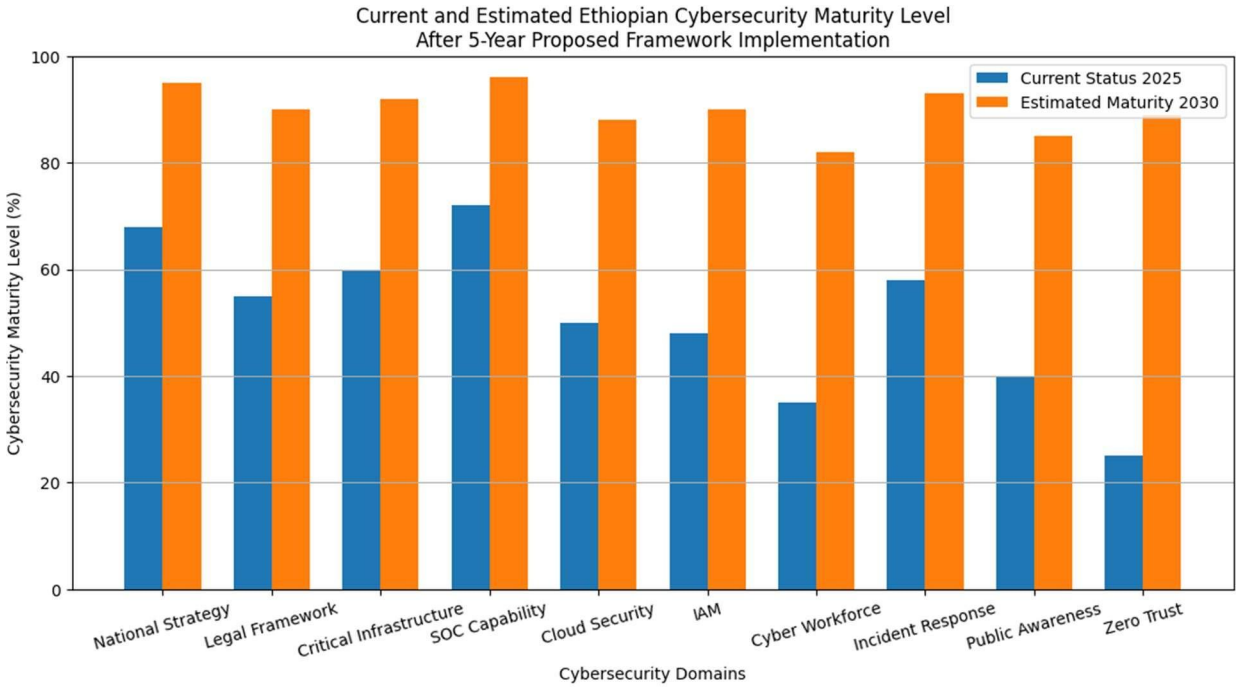

Figure 7, Cybersecurity Maturity Level of Ethiopia: Status and 5-Year Projection

8. Challenges and Advantages of Ethiopia's Digital Transformation

The digital transformation in Ethiopia propelled by the Digital Ethiopia 2030 (DE2030) strategy and the Mesob Digital Collaboration Ecosystem is a complex socio-technical transition where the advancement of technology is tied to the economic structure, institutional capacity, governance systems, and readiness of the society. This transformation involves not only digitizing services but also the reconfiguration of the relationship between the state, markets and citizens in a digitally enabled ecosystem. The process brings about a lot of potential opportunities for modernization and inclusive development, but also has structural limitations that shape the process in terms of how fast, deep, and sustainable it can be.

8.1 Challenges of Ethiopia's Digital Transformation

Ethiopia's digital transformation is a multifaceted process, where economic, political, institutional and social challenges are interdependent. Together, these dimensions create the speed and success of digital adoption nationwide.

8.1.1 Economic Challenges

One of the biggest challenges from an economic point of view is the development of digital infrastructure with high costs. There is a significant investment needed to roll out national fibre-optic networks, secure data centers, cloud IT systems, and interoperable government platforms. These investments, however, are very reliant on public funding and have a limited private sector involvement, thereby delaying digital large-scale expansion.

Furthermore, the lack of a well-developed digital private sector is another significant constraint. New fields of fintech, cloud, digital startups and other areas are still being developed, and there is still limited venture capital, innovation funds and entrepreneurial structures. This will result in a decrease in the output of innovation and in the competitiveness of the national digital economy.

In addition, Ethiopia's cash-based economy hinders the penetration of digital financial services, mobile payment and e-commerce platforms. This is further compounded by the shortage of foreign currency and dependence on imported ICT equipments which further limits the scale of technology and further delay the process of infrastructure modernization.

8.1.2 Political and Institutional Challenges

Politically and institutionally, the process of digital transformation in Ethiopia is both well coordinated at the central level and also facing implementation challenges. The centralized governance system helps to align national policies, but can also be a constraint on institutional flexibility and local innovation.

A key issue in institutions is the lack of interoperability within government systems. There is a large number of public institutions still functioning in silos with legacy, non-integrated systems. Such

fragmentation can hinder the creation of a single digital ecosystem and demands a significant level of standardization, coordination, and system harmonization for facilitating the Mesob Digital Collaboration Ecosystem.

Further, regulatory developments in sectors like financial technology, digital identity, data governance, and cybersecurity are constantly changing, leaving stakeholders uncertain. This doubt can hinder the investment decisions and delay the involvement of the private sector in digital projects.

Last but not least, political and governance stability is vital to supporting digital transformation, as any political or governance disruption can have a negative impact on digital services reliability, trust, and continuity.

8.1.3 Social Challenges

One of the biggest challenges in terms of social aspect is the constant urban–rural digital divide. Rural and urban areas lack a digital divide in terms of connectivity, as infrastructure is generally accessible, yet in terms of access to reliable internet services and digital platforms, there can be a digital divide.

Low digital literacy and inadequate ICT skills among citizens and parts of the labour force are also a significant barrier. This significantly hinders meaningful interactions with digital systems, and the impact on productivity and service of digital transformation efforts is compromised.

Further, trust, awareness and perception of digital systems, specifically data privacy, cybersecurity and digital identity, impact the uptake and trust in government and private digital systems.

Furthermore, the youth unemployment and the lack of capacity to absorb skills in the labour market are a structural issue. While there is a growing number of digitally skilled young people, the economy is not ready to make optimum use of these resources and as a result a type of underutilization of human resources.

8.2 Advantages of Ethiopia’s Digitalization and Mesob Digital Collaboration Ecosystem

The Digital Ethiopia 2030 (DE2030) Strategy and the Mesob Digital Collaboration Ecosystem offer great opportunities to modernize governance, enhance public service delivery, deepen institutional collaboration and foster economic growth in Ethiopia. The interoperability of digital systems, cloud infrastructures, digital identity platforms and common digital services facilitates efficient, transparent, secure and citizen-centric governance. The Mesob ecosystem boosts the security of data sharing, interoperability, digital innovation, and coordinated communication between institutions, and contributes to strengthening cybersecurity governance and national cyber resilience. In conclusion, digitalization facilitates Ethiopia's digital government transformation towards a modern, integrated and sustainable digital government system in line with national development goals.

8.2.1 Promoted greater efficiency and integration of government services

By unifying and interoperating the generally disjointed government systems, Ethiopia's digital transformation greatly enhances public service delivery. The Mesob platform enables the exchange of data between institutions, thereby avoiding redundant and manual processes and delays. This leads to quicker turnaround, smoother workflows and more integrated Government service delivery.

8.2.2 Strengthened transparency, accountability and governance

Digital systems enhance transparency with a traceable and auditable service processes. All transactions are recorded, time stamped and monitored digitally minimizing opportunities for corruptly and inefficiency in administration. This helps to enhance institutional accountability and public confidence in government actions by providing more transparent and reliable service mechanisms.

8.2.3 Economic Growth and Financial Inclusion

The digital ecosystem is used to facilitate economic modernization in the ease of business registration, tax and regulatory compliance. It also boosts access to finance using digital identities and payment systems resulting in greater citizenship and business participation in the formal economy. This helps promote entrepreneurship, investment and enhances national revenue collection capacity.

8.2.4 Citizen Convenience and Inclusive Access to Services

Digitalization is a solution to minimise the need for physical visits to government offices, by providing access through online platforms and one stop service centers. This saves time, will reduce costs and make the citizens more convenient. Increasing infrastructure leads to increased access to services for rural and underserved populations, increasing inclusiveness in service provision.

8.2.5 Governance and institutional modernization based on data

The Mesob ecosystem will allow sharing across institutions, aiding the evidence-based decision making and better policy formulation. Real-time and integrated data enable improved planning, monitoring and resource allocation. This improves the capacity of institutions, modernizes governance and boosts Ethiopia's competitiveness at the global level in the long-term.

9. Conclusion and Recommendations

9.1 Conclusion

The findings of this study indicate that the fast pace of digital transformation in Ethiopia as reflected in the Digital Ethiopia 2030 (DE2030) strategy has significantly enhanced the digital service delivery, institutional integration and e-government development. The adoption of the Mesob Digital Collaboration Ecosystem is a major milestone towards interoperable, integrated and citizen-centered digital governance. But with ever increasing interconnection of digital systems comes complex cybersecurity issues that call for a more structured and context-specific security approach.

Research findings validate that other cybersecurity regulations, including NIST, ISO/IEC 27001, and COBIT, are not comprehensive enough to meet the needs of Ethiopia's digital governance context. They are developed without a high level of contextual adaptation to address issues of interoperability, institutional fragmentation and evolving cyber threats in digital ecosystems in developing countries. Therefore, there is a clear demand for a context-aware cybersecurity framework for Ethiopia which considers the country's technological, institutional and regulatory context.

This framework seeks to bridge these gaps with adaptive security mechanisms, IDAM, ongoing monitoring, threat intelligence and governance. The results of the research show that such a method could greatly boost cybersecurity resilience, increase system interoperability, and boost the Confidentiality, Integrity, and Availability (CIA) of digital systems. The study thus concludes that the Mesob Digital Collaboration Ecosystem needs to be secured by a context-aware cybersecurity framework for sustaining digital transformation in Ethiopia.

9.2 Recommendations

The results of this study have a number of key recommendations to promote effective implementation of the cybersecurity framework and enhance Ethiopia's cyber resilience:

- The government should develop a national cybersecurity framework for digital platforms with specific consideration to the context, in line with the Digital Ethiopia 2030 strategy, to ensure uniform cybersecurity for all digital infrastructure.
- Effective institutional coordination mechanisms should be developed to enhance the cooperation between the ministries, agencies and regional administrations in the field of cybersecurity governance.
- Investment in cyber security infrastructure such as Security Operations Centers (SOC), SIEM systems, and national monitoring platforms should be given priority.
- It is necessary to develop continuous capacity building and cybersecurity training programs to cope with the shortage of skilled people in cybersecurity.
- Government cybersecurity policies and interoperability frameworks should be standardized and adopted throughout all government systems to minimize fragmentation.
- Enhance access control and limit the access to systems by implementing Identity and Access Management (IAM) and Zero Trust security models.
- Awareness programs for the use of the internet and computer and cyber hygiene should be implemented in government institutions to increase the cyber literacy of government officials and citizens.

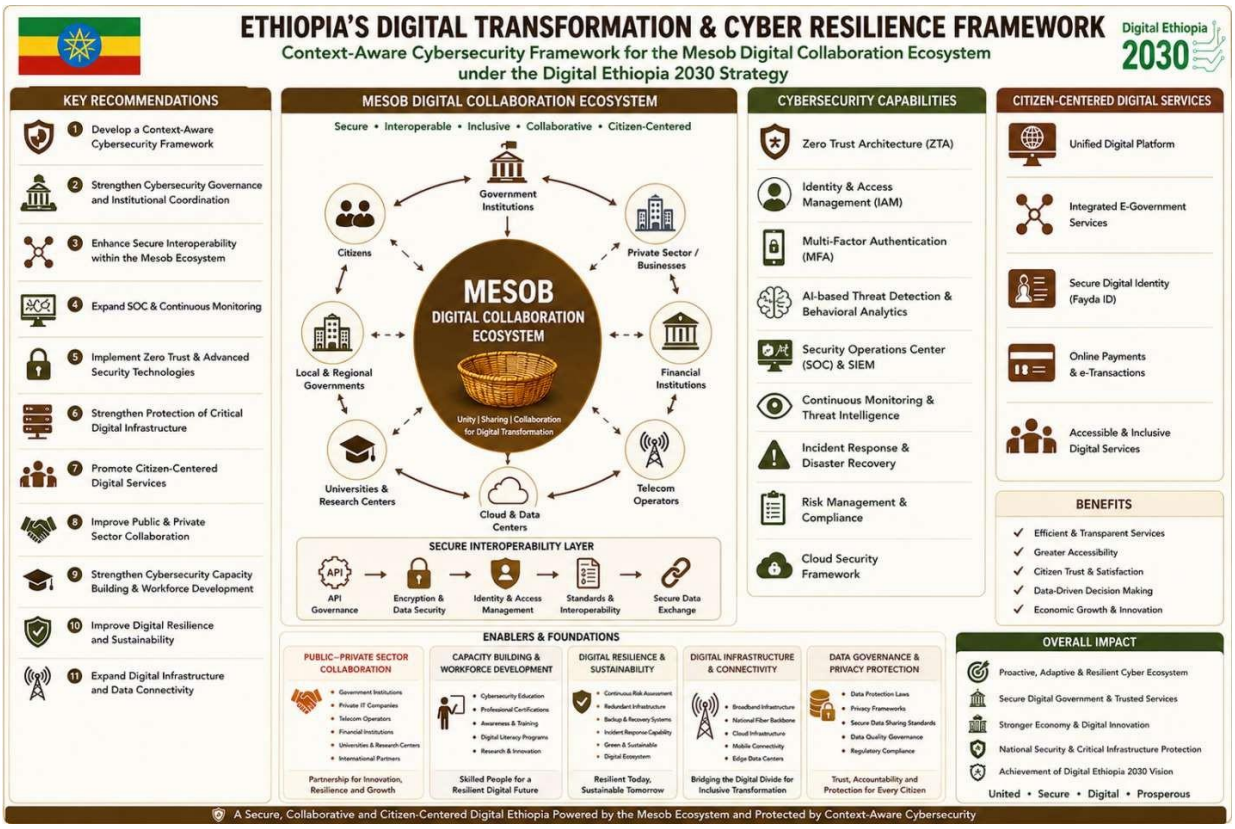

Figure 8, Recommended Ethiopia's Digital Transformation and Cyber Resilience Framework

9.3 Future Research Directions

While this study offers a detailed cybersecurity landscape for Ethiopia's digital economy, there are several aspects that need further research to improve and broaden the applicability of the cybersecurity framework for the digital economy of Ethiopia:

- Further research is needed on the applying and testing of the proposed cybersecurity framework in government institutions in the real world.
- Research to integrate Artificial Intelligence (AI) and Machine Learning (ML) for predictive cybersecurity and automated threat detection is required.
- More research is needed in the area of a blockchain security scheme to enhance information integrity and trust in digital governance systems.
- Advanced Zero Trust Architecture (ZTA) models specific to the Ethiopian context in the Mesob ecosystem should be studied.
- More research is needed on cyber security policy implementation models and regulations to help with compliance at the national level.
- Furthermore, future research should look at the socio-technical effect on cybersecurity uptake, focusing on user behavior changes, institutional readiness and organizational change management.

In conclusion, this research validates the need for a different approach to cybersecurity to achieve Ethiopia's digital transformation. It needs a nation integrated, adaptive and context-aware cybersecurity framework with a digital governance structure that promotes interoperability and enhances long-term cyber resilience in the Digital Ethiopia 2030 vision.

References

[1] Ministry of Innovation and Technology (MinT), *Digital Ethiopia 2030: A Strategy for Ethiopia's Inclusive Prosperity*. Addis Ababa, Ethiopia, 2020.

[2] Federal Democratic Republic of Ethiopia (FDRE), *Digital Transformation Strategy of Ethiopia 2030*. Addis Ababa, Ethiopia, 2020.

[3] Ethiopian Artificial Intelligence Institute (EAII), *National Artificial Intelligence Strategy for Ethiopia*. Addis Ababa, Ethiopia, 2023.

[4] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, Gaithersburg, MD, USA, 2018.

[5] ISO/IEC 27001, *Information Security Management Systems — Requirements*. Geneva, Switzerland: International Organization for Standardization, 2022.

[6] ISO/IEC 27002, *Information Security Controls*. Geneva, Switzerland: International Organization for Standardization, 2022.
[7] European Union Agency for Cybersecurity (ENISA), *Zero Trust Architecture: Principles and Concepts*. European Union, 2021.
[8] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020.
[9] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, Cambridge, MA, USA, 2010.
[10] Microsoft Security, *Zero Trust Deployment Guide*. Microsoft Corporation, Redmond, WA, USA, 2022.
[11] M. J. Covington, W. Long, S. Srinivasan, A. Dev, M. Ahamad, and G. D. Abowd, "Securing Context-Aware Applications Using Environment Roles," in *Proc. 6th ACM Symposium on Access Control Models and Technologies*, Chantilly, VA, USA, 2001, pp. 10–20.
[12] J. B. Hong, D. S. Kim, and T. H. Kim, "Context-Aware Security Framework for IoT Environments," *Future Generation Computer Systems*, vol. 76, pp. 314–324, 2017.
[13] M. S. Al-Kahtani and R. Sandhu, "A Model for Attribute-Based User-Role Assignment," in *Proc. Annual Computer Security Applications Conference (ACSAC)*, Las Vegas, NV, USA, 2002, pp. 353–362.
[14] United Nations Department of Economic and Social Affairs (UNDESA), *United Nations E-Government Survey 2024: Digital Government for Sustainable Development*. New York, NY, USA: United Nations, 2024.
[15] World Bank, *GovTech Maturity Index: The State of Public Sector Digital Transformation*. Washington, DC, USA: World Bank, 2022.
[16] Organisation for Economic Co-operation and Development (OECD), *Digital Government Index: 2019 Results*. Paris, France: OECD Publishing, 2020.
[17] Cloud Security Alliance (CSA), *Security Guidance for Critical Areas of Focus in Cloud Computing*, 2021.
[18] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2011.
[19] IBM Security, *AI and Cybersecurity Report*. IBM Corporation, Armonk, NY, USA, 2023.
[20] MITRE Corporation, *MITRE ATT&CK Framework*. Bedford, MA, USA, 2024.
[21] Gartner, *Emerging Technologies in Cybersecurity and AI-Driven Threat Detection*. Stamford, CT, USA, 2023.
[22] African Union, *The Digital Transformation Strategy for Africa (2020–2030)*. Addis Ababa, Ethiopia, 2020.
[23] Smart Africa Alliance, *African Digital Government and Cybersecurity Report*. Kigali, Rwanda, 2022.
[24] International Telecommunication Union (ITU), *Global Cybersecurity Index 2023*. Geneva, Switzerland, 2023.
[25] Information Network Security Administration (INSA), *National Cybersecurity Capacity Building Initiatives in Ethiopia*. Addis Ababa, Ethiopia, 2023.
[26] Ethiopian Communications Authority (ECA), *National ICT Infrastructure and Digital Connectivity Framework*. Addis Ababa, Ethiopia, 2022.
[27] National Bank of Ethiopia (NBE), *Digital Financial Services and National Payment Systems Strategy*. Addis Ababa, Ethiopia, 2023.
[28] IEEE Transactions on Information Forensics and Security, IEEE Publications.
[29] *Computers & Security*, Elsevier Publications.
[30] *Journal of Cybersecurity*, Oxford Academic Publications.
[31] *Government Information Quarterly*, Elsevier Publications.
[32] *International Journal of Information Security*, Springer Publications.
[33] *Future Generation Computer Systems*, Elsevier Publications.
[34] *Journal of Information Security and Applications*, Elsevier Publications.