Digital Government Strategy 2025-2030

Advancing a Connected, User-Centred, Data-Driven, Environmentally-Responsible and Secure Digital-First Government

Connected | User Centred | Data-Driven | Environmentally Responsible | Secure





Foreword by the Prime Minister

Ethiopia is at a tipping point of transformation; digital technologies will catalyse our sustainable development journey. Our Home-Grown Economic Reform Agenda highlights the importance of digital technologies as a pillar of growth next to the agriculture, manufacturing, tourism, mining, and creative industries sectors.

Guided by the Digital Ethiopia 2025 Strategy, we have taken several steps to make digital technologies integral to our economy. The opening of the telecommunication sector for competition, expansion of digital services across the government, especially in the health, education, economic planning, and management sectors, the launch of a Digital Identity (Fayda) programme and increasing adoption of mobile banking by our citizens are among recent gains contributing to Ethiopia's digital economy journey. We have also integrated emerging and disruptive technologies, such as Artificial Intelligence and Spatial Data Infrastructure, into our development efforts. I am strongly convinced that emerging technologies like AI, the Internet of Things, blockchain, and cloud computing will provide us with unprecedented opportunities for improved government, accelerated agriculture and food security, good health and well-being, clean energy, industrial and infrastructure development and innovation.

At the same time, we realise the challenges and opportunities, especially the need to accelerate access to infrastructure and digital literacy of citizens more critically the importance of creating an enabling environment for Ethiopia's emerging digital economy ecosystem. A core potential of digital technologies is accelerating job creation; therefore, we need to upskill our people, especially our youth, with the latest digital technology concepts and tools to ensure everyone in Ethiopia can leverage information and communication technologies for improved quality of life. Progress in the gig economy, like ride-sharing, has already shown that digital tools are transforming the old way of doing things; thus, skills are paramount for innovating new software products and, more generally, for thriving in the digital economy. We must also update our regulatory frameworks and ensure financial and technical incentives are available for innovative digital entrepreneurs.

National digital transformation begins with a transformed government. Increased adoption of digital and emerging technologies within the public sector is key to achieving our economic prosperity and serving citizens, businesses and visitors more effectively and efficiently.

This Digital Government Strategy recognises the importance of a connected government, where we build shared infrastructure and reuse data and applications, achieve a user-centred government in which we commit to providing impactful and easy-to-access

services. We need to establish a zero-trust secure government and share and leverage data for effective decision-making and economic value addition. Our commitment to a data-driven and customer-centric government requires that all public institutions coordinate and interoperate within a “whole of Government” framework, adhering to standards and a government enterprise architecture.

Achieving a connected, data-driven, open, and secure government requires improving our skills, raising citizens’ awareness of the opportunities and challenges of digital technologies, and collaborating and coordinating at local, zone, regional, and federal levels. We should align digital and emerging technologies with our government transformation. At the same time, we should reform our archaic business processes to leverage technology to deliver better services. Therefore, I call upon public and private institutions and partners to actively participate and support our digital government journey.

Foreword by Minister of Innovation and Technology

Digital technologies have become important tools for learning, delivery of government services and financial inclusion. They are increasingly becoming part of day-to-day communication, information exchange and empowerment. The COVID-19 pandemic has fuelled the expansion of digital services worldwide, with citizens and businesses now demanding online services and cashless payments. Ethiopia has seen increased digital technology and e-payment usage over the last few years, spurring a broader digital transformation journey in our country.

The Government realises that investment in digital technologies is important to growth and prosperity. We have adopted Digital Ethiopia 2025, which guides us through digital technology investment halfway through the ten-year National Development Plan. Digital Ethiopia 2025 is hinged on four core objectives:

- harness opportunities presented by digitalisation to support Ethiopia's broader development objectives,
- create a sense of urgency and mobilise stakeholders to address digitalisation constraints and take hold of opportunities,
- provide the basis to coordinate and strengthen existing digitalisation initiatives, and,
- contextualise Ethiopia's digitalisation journey within a global context.

The Government has been creating the foundations for digital development. So far, we have invested in several infrastructures and ICT services projects – namely WoredaNet, which connects districts to central government; SchoolNet and EthERNet, which links schools, colleges and universities to modern applications, National Data Centre, e-Services Portal, and a multitude of sector-specific information systems, especially in health, education, agriculture and public financial management. We have also been investing in ICT in government to advance our public sector automation. Our public offices increasingly use ICTs to provide services to citizens and businesses. The reform in the communication sector has also spurred competition and innovation in many aspects of digitalisation.

We are also mindful that our journey towards digitalisation is just beginning. There is a need to accelerate access to infrastructure and services, improve the skills of citizens, and ensure that our enterprises become competitive in the digital economy. The modernisation of government is another area of our attention. We need to improve coordination to move towards an interconnected government at the federal and regional levels. Our vision for 'digital first', data-driven and a whole-of-government approach is inherent in this. We need to create platforms that improve the exchange and sharing of data between government entities.

The Digital Government Strategy and Implementation Roadmap, drafted through extensive consultative effort, will be an important tool that will guide us on that journey. I would like to thank the European Union for funding this important initiative. I wish to extend my deepest appreciation to my staff, other Ministries, Departments, Agencies, regional government experts and stakeholders who participated in different consultation meetings and provided relevant information leading to the development of the Digital Government Strategy and Implementation Roadmap. I also call upon all stakeholders to support the implementation process.

Acknowledgements

The Digital Government Strategy and Implementation Roadmap and the Enterprise Architecture were commissioned by the Government of the Federal Democratic Ethiopia and funded by the European– Project No. 300052766 – SIEA-2018-14397.

His Excellency Dr Belete Molla, Minister of Innovation and Technology , guided the development of the Strategy and Implementation Roadmap and Enterprise Architecture. The Project has also benefited from the Support of Dr Yeshurun Alemayehu, State Minister for Innovation and Technology. Dr Abiot Sinamo, Chief Executive Officer of National Electronic Government Development, oversaw the project. Dr Abiot Bayou, Senior Advisor to the Minister of Innovation and Technology, provided substantive comments and guidance.

The Ministry of Innovation and Technology counterpart team that provided ongoing coordination and substantive support included Admas Mamo, Biruhtesfa Taye, Dr Fekade Getahun, Helen Mergia, Tewodros Tazeze, Miftah Jemal, Babesha Kenaw, Meklit Teshome and Bethlehem Bedilu. We thank them all for their dedication and ongoing support in bringing this project to fruition. The Digital Government Strategy and Implementation Roadmap have also benefited from the consultation and guidance of different government institutions, the private sector, academia and development partners, who have provided invaluable input and feedback.

The Strategy and Implementation Roadmap and the GEA have also benefited from the consultation and guidance of the EU Delegation in Ethiopia. Ioana Albulescu and Leul Habte provided the project's overall coordination and substantive guidance. We appreciate the European Union Delegation's support.

The analysis and writing of the Strategy and Implementation Plan and the Government Enterprise Architecture was carried out by a team of consultants managed by the DT Global Consortium. Dora Gombocz of DT Global, Lluis Palau Meseguer of OCA Global, and Vesna Kahrimanovic of DAI provided the coordination and technical support for the project. Dr Lishan Adam (Team Leader), Samuel Chari, Dr Mweene Monze, Dr Constantine Bitwayiki, Vladimir Abramytchev, Mouad Boumahdi, Abraham Kibret, Gezahegn Chalchisa and Messay Hailemariam conducted the baseline survey, analysis and writing.

Contents

List of Tables

List of Figures

Abbreviations

Term	Description
AAU	Addis Ababa University
AfCFTA	Africa Continental Free Trade Area
AI	Artificial Intelligence
AIMS	African Institute of Mathematical Studies
API	Application Programme Interface
BCP	Business Continuity Plan
BEIC	Business Environment and Investment Climate, including eGovernment
BPR	Business Process Reengineering
CDR	Call Detailed Record
CDO	Chief Data Officer/ Chief Digital Officer
CERT	Computer Emergency Reporting Team
CGSI	Core Government Service Index
CII	Critical Information Infrastructure
CIO	Chief Information Officer
CTO	Chief Technology Officer
DDR	Data Detailed Record
DGRA	Digital Government Readiness Assessment
DGSC	Digital Government Support Centre
DIAL	Digital Impact Alliance
DIAP	Detailed Implementation Action Plans
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
EAF	Enterprise Architecture Framework
ENEAF	Ethiopia National Enterprise Architecture Framework
EGIF	Ethiopian Government Interoperability Framework
EGDI	eGovernment Development Index
eIDAS	Electronic Identification, Authentication and Trust Service
EMIS	Education Management Information System
EoDB	Ease of Doing Business
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
ETA	Ethiopian Telecommunication Authority
EU	European Union
FCSC	Federal Civil Service Commission

G2B	Government to Business
G2C	Government to Citizens
G2G	Government to Government
GCI	Global Cybersecurity Index
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GEA	Government Enterprise Architecture
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
GoE	Government of Ethiopia
GTEI	GovTech Enablers Index
GTI	Government Transformation Index
GTMI	GovTech Maturity Index
GWAN	Government-Wide Area Network
HCI	Human Capital Index
HGER 2.0	Home Grown Economic Reform 2.0
HMIS	Health Management Information System
HRMS	Human Resources Management System
IaaS	Infrastructure as a Service
ICT	Information and communications technology
ID	Identity
IFMIS	Integrated Financial Information Management System
INSA	Information Network Security Administration
IoT	Internet of Things
IP	Internet Protocol
IPDR	Internet Protocol Detail Record
ISO	International Standards Organization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunications Union
LAN	Local Area Network
LDC	Least Developed Countries
Mbps	Megabits Per Second
MCIT	Ministry of Communication of Information Technology
MDA	Ministries, Departments, and Agencies
M&E	Monitoring and Evaluation
MInT	Ministry of Innovation and Technology (Ethiopia)
NDC	National Data Centre
NEAF	National Enterprise Architecture Framework

NREN	National Research and Education Network
OCR	Optical character Recognition
OECD	Organization for Economic Cooperation and Development
OSI	Online Service Index
PaaS	Platform as a Services
PDSI	Public Service Delivery Index
PKI	Public Key Infrastructure
PMO	Project Management Office
PPP	Public and Private Partnerships
PWC	Price Waterhouse Coopers
R&D	Research & Development
REST	Representational State Transfer
SaaS	Software as a Services
SD-WAN	Software-defined Wide Area Network
SDG	Sustainable Development Goals
SDI	Spatial Data Infrastructure
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SQT	Software Quality Testing
STEM	Science, Technology Engineering and Mathematics
TTI	Telecom Infrastructure Index
TYDP	Ten Year Development Plan
UNDESA	United Nations Department for Economic and Social Affairs
UNESCO	United Nations Education Scientific and Cultural Organisation
UX/UI	User Experience/ User Interface
VoC	Voice of Customer
WB	World Bank
WCAG	Web Content Accessibility Guide

Executive Summary

This Strategy charts a path for Ethiopia's transition from delivering basic eGovernment services to a full-fledged Digital Government where procedures will be digital by default, services become more user-centred, and emphasis is placed on data, emerging technologies and sustainable ecosystem- with a whole-of-government approach at the core. The Digital Government Strategy envisions a connected, user-centred, data-driven and secure government that delivers end-to-end shared digital public service within the public sector and to citizens, businesses and visitors. The transition from basic eGovernment services to a whole-of-government digital public service will be achieved through actions in four major areas:

- Digital Government Applications and Services: This comprises extending back-office automation, accelerating shared applications and eServices, transforming access channels and fostering digital government building blocks like ID, vehicle, property, address and land registries, payment systems and creating an Enterprise Service Bus.
- Digital Government Foundations—encompassing the modernisation of digital government infrastructure (cloud, GWAN, computing and software resources), upgrading government enterprise architecture, integrating emerging technologies, advancing data management and sharing, and fostering the enterprise and research ecosystem.
- Digital Government Enablers encompass coordination and governance frameworks, legal frameworks, cybersecurity frameworks, administrative reform and change management, digital inclusion and e-participation.
- Digital Government Essentials – which include financing and regional and global coordination.

The strategy proposes 60 major activities in 14 digital government mission areas under the four pillars shown in the Table below.

Pillars	Mission Areas
Digital Government Core	Application and Services
Digital Government Foundations	Digital Infrastructure
	Data Management, Governance and Use
	Enterprise Architecture
	Emerging Technologies
	Enterprise and research ecosystem development
Digital Government Enablers	Coordination and governance
	Legislative framework
	Cybersecurity and business continuity
	Reform and change management
	Skills and culture
	Inclusion and eParticipation
Digital Government Essential	Financing
	Regional and international cooperation

The sixty activities will be implemented through detailed action plans, the outcomes of which will be measured using Key Performance Indicators in line with the United Nations eGovernment Development Index (EGDI) and the World Bank's GovTech Maturity Index metrics.

The Implementation Roadmap envisages a funding requirement of US$60 million to implement the activities, exclusive of network infrastructure, equipment, applications and human resources. Mobilisation funding and establishing a digital government support centre are recommended at the beginning of this Strategy because they are critical for the transition from eGovernment to a full-fledged digital government in Ethiopia.

Part I: Digital Government Progress in Ethiopia

1 Introduction

Digital technologies, including computers, the Internet, mobile devices and disruptive technologies like artificial intelligence, blockchain and the Internet of Things, are transforming how governments do business, interact with citizens and deliver services. These technologies have changed how people work, live, and engage with each other, as well as the environment and government. Governments are leveraging digital and emerging technologies to be accountable and less bureaucratically burdensome.

Digital and advanced emerging technologies promise to accelerate the achievement of globally agreed-upon Sustainable Development Goals (SDGs), from ending extreme poverty to reducing maternal and infant mortality, promoting sustainable farming and decent work, and achieving universal literacy. They are key in attaining the African Union Agenda 2063 and Ethiopia's national development aspirations.

The Government of Ethiopia recognises the role of digital and emerging technologies. ICTs have been integral parts of Ethiopia's development plan. The Homegrown Economic Reform Agenda, Ten Years Development Plan (2021-2030) and Digital Ethiopia 2025 lay out the Government's plan to leverage these technologies for social and economic development and job creation. The Homegrown Economic Reform Agenda[1] emphasises sector reform, acceleration of digital government services and electronic commerce, digital skills and digitalisation of the financial and logistics sector. The Ten-Year Development Plan pays particular attention to the agricultural, manufacturing, mineral, tourism, and Information and Communication Technology sectors as sources of growth. Digital Ethiopia 2025[2] emphasises ICT use in priority sectors (Agriculture, Manufacturing and Services), infrastructure development, digital Identity, jobs creation, boosting forex earnings and inclusive prosperity.

COVID-19 has shown the importance of being digital and leveraging these technologies as fast as possible to deliver many government services. It has also indicated the need to speed up digitalization to address emergencies and alleviate citizens' and businesses' information gaps. Ethiopia's future competitiveness partly lies in the speed and capacity at which it embraces digital and emerging technologies.

Many Ethiopians still are not connected to the digital world, and a few who access the Internet use online public services. Data from Research ICT Africa shows that in 2023, only about 4% of the population has some contact with digital government services, such as using mobile banking to pay for tax services. The study also shows an ever-growing use of social media in Ethiopia for entertainment and news, less for digital government,

[1] A Homegrown Reform Agenda, Unlocking Ethiopia's Economic Potential, https://www.mofed.gov.et/media/filer_public/0e/4c/0e4c0c11-8262-4e53-b395-0b1c0aa26976/ethiopia-_economic_reform_agenda_.pdf

[2] Government of Ethiopia, Digital Ethiopia, https://www.lawethiopia.com/images/Policy_documents/Digital-Ethiopia-2025-Strategy-english.pdf

education or other tangible services. This growing appetite for digitally-enabled interaction suggests that the government can harness the power of information and communication technologies and other disruptive technologies to provide efficient services for citizens and businesses.

1.1 Background to the Development Digital Government Strategy and Implementation Plan

The Government of Ethiopia has been implementing digital public services projects for the last two decades, beginning with the National ICT Strategic Plan and an ICT for Development (ICT4D) Action Plan for 2006 – 2010, followed by two eGovernment Plans, one between 2011-2015 and the next between 2016-2020.

- Under the 2006 – 2010 Strategy, the Government Information System Development and Data Centre Administration team of the then Ministry of Communications and IT (MCIT) developed and managed projects that targeted integrated information systems in the public sector. The integrated information systems enabled initial government services delivery on the web; however, gaps existed in the transition to full-fledged online services. Then, the Ministry of Communications and IT engaged PricewaterhouseCoopers Pvt—Ltd (PwC). to develop the National eGovernment Strategy and Implementation Plan.
- The 2011-2015 eGovernment Strategy was written by PwC and focused on customer-centric services delivered seamlessly and conveniently. It also defined a governance structure, including establishing a Project Management Office to support the implementation of the strategy. The strategy selected 219 services to be digitised in a phased approach. These services were to be available to the public through a national e-portal, call centre, ICT service centres and mobile application. The delivery was planned to be facilitated and strengthened through six core projects – National Payment Gateway, Enterprise Architecture Framework, Public Key Infrastructure, National Data Set, National Enterprise Service Bus and National Integrated Authentication Framework. Additionally, common applications that cut across all ministries were proposed, including eProcurement, Human Resource Management System, eOffice, email, and Integrated Financial Management and Information Systems (IFMIS).
- The 2016 – 2020 eGovernment Strategic Plan, developed by KPMG, focused on addressing the gaps in the earlier strategy and enhancing the eGovernment programs to generate more value for citizens and businesses. The Strategy emphasised promoting an enabling environment for eServices, enhancing

government e-readiness, increasing usage, and defining the operating model. Other areas of attention included establishing an efficient and transparent governance structure, innovations in eGovernment services, promoting entrepreneurship through ease of doing business, and leveraging SMART technology-driven initiatives.

Ethiopia's effort to promote effective eGovernment services throughout 2006-2022 saw improved access to digital tools in the public sector. Still, progress in the use of digital public services remained very low. Institutions continued to operate in silos without sharing resources, and similar infrastructure and services were implemented by different Ministries, Departments and Agencies (MDAs) that resulted in duplication of efforts.

Data from e-services.gov.et shows there were 350 e-services with 244,000 registered users. This is very low compared to the online population. Users' uptake of the services was low due to limited awareness among the population about the services available on the different MDA portals and inadequate user focus on the design of the online services. The proposed Project Management Office (PMO) was not established; therefore, the monitoring and evaluation framework needed to be fulfilled to ensure follow-up and assessment of the eGovernment initiatives. The governance structure was not implemented either, leading to continued siloed implementation of the different eGovernment initiatives by MDAs and regional governments.

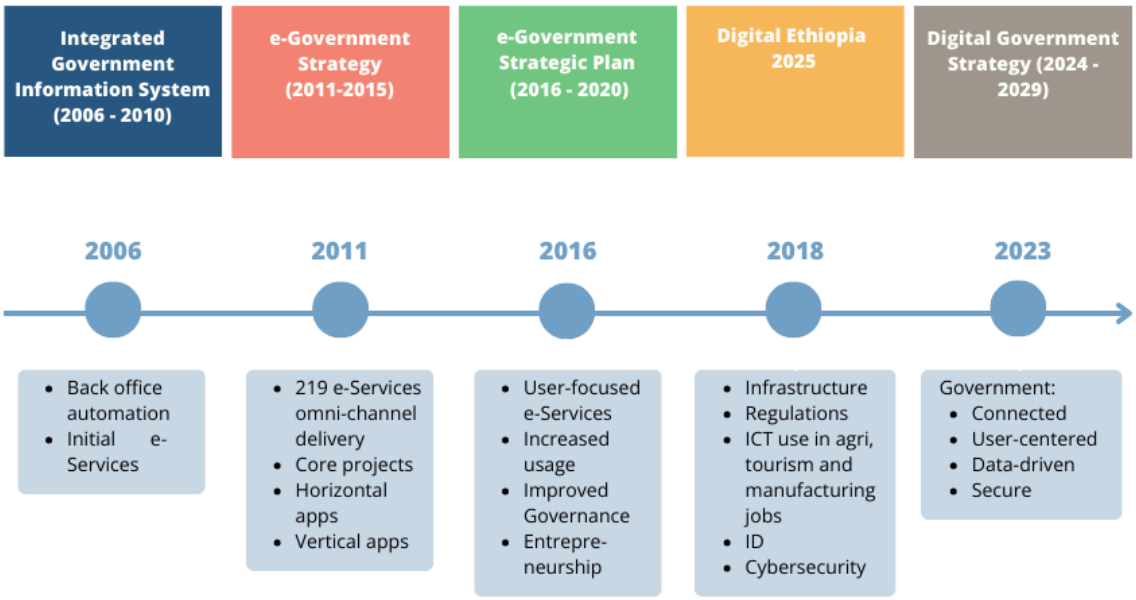

Figure 1: E-Government Evolution in Ethiopia

A situation review shows that the Government of Ethiopia (GoE) has made some progress in improving mobile payments and issuing digital IDs. There is still a lot to do in leveraging identity for digital public services and integration and sharing of address registries, business registries and land registries that are critical for successful digital government. Progress in shared services has been facilitated by launching an Integrated Financial Management Information System and e-procurement systems. However, efforts in e-

office implementation, including document management, exchange and messaging and government open data, were slow.

A comparative analysis of eGovernment strategies' themes shows a wider gap between Ethiopia's effort and what has been achieved in other leading countries.

Table 1: Comparative Analysis of Themes in Ethiopian E-Government Strategy and Strategies of Other Countries

Main Themes of Ethiopian eGovernment Strategies	Themes of Current Digital Government Strategies in Other Countries
E-services enablement – MDA eServices and application, Horizontal Applications, Common Application **Core projects - National Payment Gateway, Enterprise Architecture Framework, Public Key Infrastructure, National Data Set, National Enterprise Service Bus and National Integrated Authentication Framework** **Service channels** **Enablers – capacity building, marketing and awareness, policies and standards, monitoring and evaluation, public and private partnership** **2016-2020 eGovernment Strategic Plan** **Infrastructure – data centre, network** **Enterprise architecture** **Regulatory framework** **Public, private partnership** **Change management** **e-services and government portal** **channels** **Skills and awareness**	e-Services classification, design, prioritisation and implementation Building and sharing foundational registries (ID, business registries, address registries, land registries, vehicle registries) Secure IT infrastructure Trust, security and privacy Governance and organizational Architecture for Digital Government Coordination Legal and regulatory framework Digital capabilities and skills Data strategy – data culture and leadership, data governance, staff and capability, data release, sharing and use, data analytics and visualisation (e.g., Australia) Research and innovation in digital government Change management and business process design Cooperation and partnership with academia and the private sector Coordination, implementation, monitoring and evaluation Financing Integration of emerging technologies

Based on the comparative analysis of themes of digital government in other countries shown in Table 1, there is a need to focus on the following areas:

- Creation, expansion and sharing of robust eGovernment registries – (digital Identity, address registry, business registry, geospatial registry of land and buildings) –

- Promotion of accelerated access to secure and affordable connectivity for citizens, businesses and government entities,
- Improving the local tech ecosystem to support eGovernment development in Ethiopia,
- Accelerating awareness and digital literacy of the population and digital skills for civil servants, government IT workforce and graduates,
- Introducing agile governance and institutional model,
- Integration of emerging technologies in eGovernment, and
- Ensuring that adequate funding is available for eGovernment projects.

1.2 Ethiopia's Scores of Global Digital Government Indices

International scores of Ethiopia's progresses in digital government indicate that despite the efforts in designing and implementing a series of eGovernment strategies, the uptake of eGovernment still needs to be higher. The recent eGovernment Development Index (EGDI), a biennial benchmarking report published in 2024 by the United Nations Department of Economic and Social Affairs, ranked Ethiopia 169th out of 193 countries on eGovernment and 166th on e-Participation. Ethiopia received an overall EGDI score of 0.3111, less than half the global average of 0.6382 and 30% below the African continent average of 0.4054. Ethiopia scored 0.373 on the Online Service Index (OSI), which evaluates the government's online services. It scored 0.501 on the Telecommunication Infrastructure Index (TII) and 0.3364 on the Human Capital Index (HCI).

Figure 2 shows that Ethiopia's eGovernment scores only improved marginally between 2014-2022. The EGDI ranking has declined since 2018 due to limited activities in expanding user-centred eServices. Projects that began in the 2010s stalled during the change of government in 2018, slowing eServices delivery amid the restructuring of the ministry responsible for the digital economy and other government entities. The frequent restructuring of MDAs did not help in the design and delivery of effective and efficient government services.

Source: Based on United Nations Department for Economic and Social Affairs EGDI data

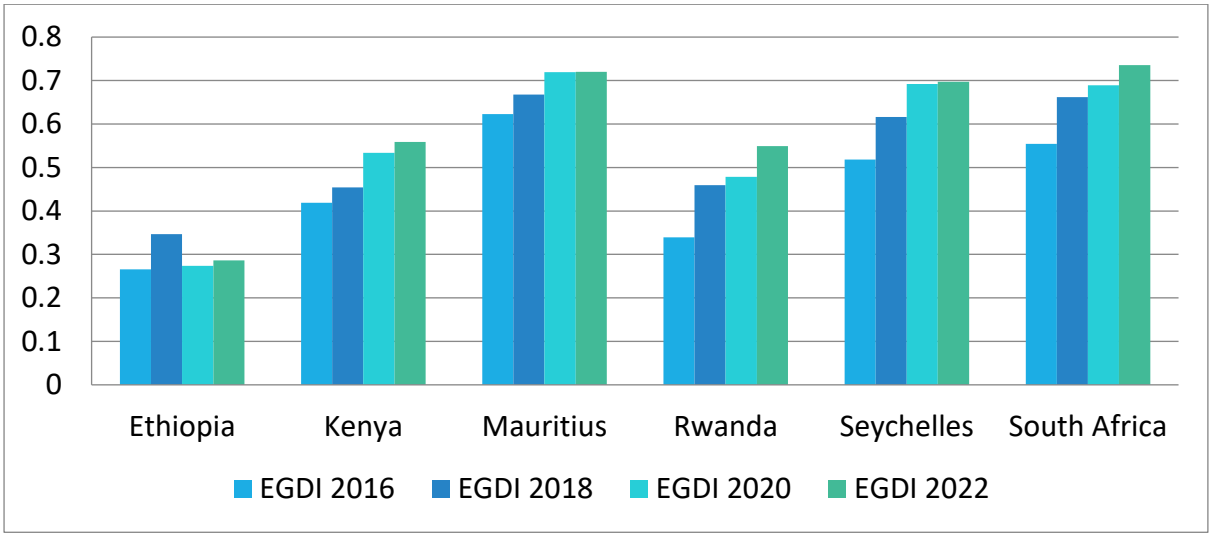

Figure 2: Evolution of EGDI in Ethiopia and Selected African Countries

More recent World Bank reviews show the potential for improvement in Ethiopia's digital public services due to the growing adoption of mobile and online payment services. Ethiopia scored 0.58 on the World Bank's Government Technology Maturity Index (GTMI) in 2022, above most of the countries in eastern and southern Africa but below regional leaders like Mauritius, Tanzania and Uganda. The GTMI is the simple average of the normalised scores of four components: the Core Government Systems Index (CGSI), based on 17 indicators; the Public Service Delivery Index (PSDI), based on nine composite indicators; the Digital Citizen Engagement Index (DCEI), based on six indicators; and the GovTech Enablers Index (GTEI), based on 16 indicators.[3]

Ethiopia's core GTMI score, which was 0.336 in 2020, has jumped to 0.58 due to increased attention to improving Core Government Systems (e.g., the Debt Management System, eProcurement Portal, Tax management system and Customs Management System). Still, progress in public services delivery, digital citizens' engagement, and GovTech enablers has remained relatively the same since 2022.

The EGDI and GTMI indices scores indicate that governments' digital agenda continues to evolve as global trends and public expectations change; thus, it is important to update eGovernment initiatives in Ethiopia based on the global lessons in core government systems design, public service delivery and GovTech enablers like shared building blocks. Building on achievements so far, the next step in digital technology use in government is to gradually graduate from "eGovernment" stage towards a "digital government" stage, where procedures are digital by design, services become more user-centred, and emphasis is placed on data and emerging technologies- with a whole-of-government

[3] World Bank, GovTech Maturity Index, Regional Brief: Eastern and Southern Africa, https://openknowledge.worldbank.org/server/api/core/bitstreams/ff1c2057-9dd3-4021-8a30-957e371d97a9/content

approach at the core. For this reason, Ethiopia needs to upgrade its terminology from "eGovernment Strategy" to a "Digital Government Strategy" where:

- Emphasis is placed on a whole-of-government/connected approach and the transformation of government as a platform,
- Every procedure in government becomes digital and designed based on users' and businesses' journeys,
- Data, including open data, drives the effectiveness and efficiency of public service,
- Efforts are increased to ensure the universal availability of open and secure digital public services to all citizens and businesses.

The transition from eGovernment to digital government also ensures the adoption of new data-driven technologies such as Artificial Intelligence (AI) and blockchain and applications such as those providing geospatial/location data for policy design and service delivery.

Source: Adapted from World Bank, 2020, GovTech: The New Frontier in Digital Government Transformation

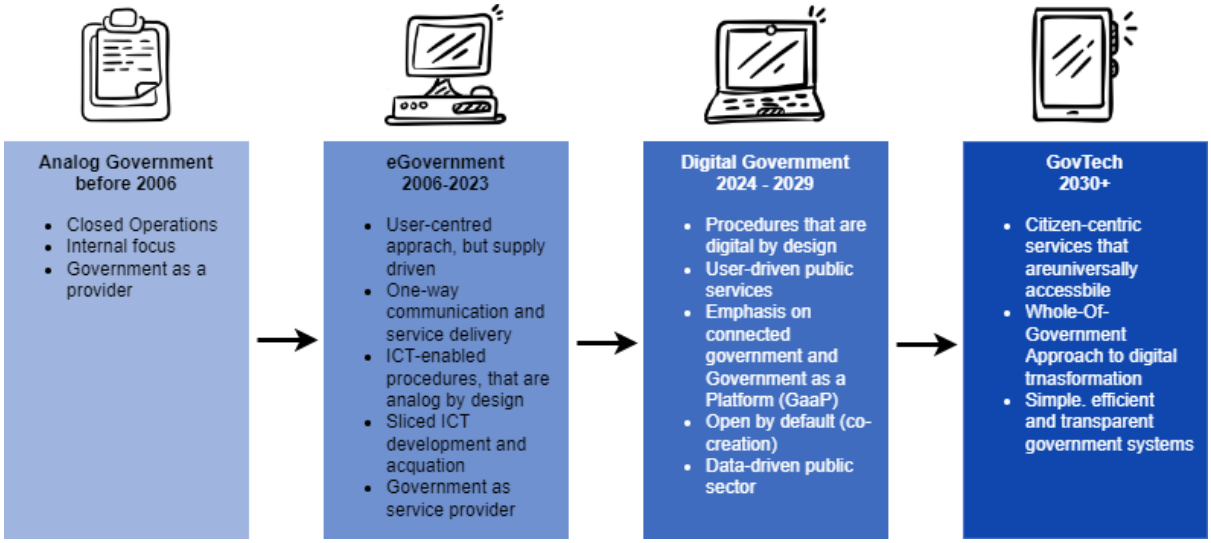

Figure 3: Ethiopia's path towards Digital Government and GovTech

Ultimately, Ethiopia should graduate to the GovTech stage (i.e., at the end of its current digital government strategy). GovTech is an advanced public sector modernisation emphasising a complete whole-of-government approach and a universally accessible, citizen-centric, efficient, and transparent government system.

2 Rationale of Digital Government

2.1 Benefits of Digital Government

Digital technologies have a wide range of benefits for the government, from providing efficient public services, increasing citizens' participation, enhancing collaboration between different public administration branches, reducing costs, and improving internal efficiency and productivity. Studies show that digital government development can promote Gross Domestic Product (GDP) growth based on some indicators, such as increased labour productivity in the public sector, increased public sector gross output, and public administration efficiency. A European study on developing digital governments in European Union member states accelerated GDP growth by two per cent from 2005 to 2010.[4]

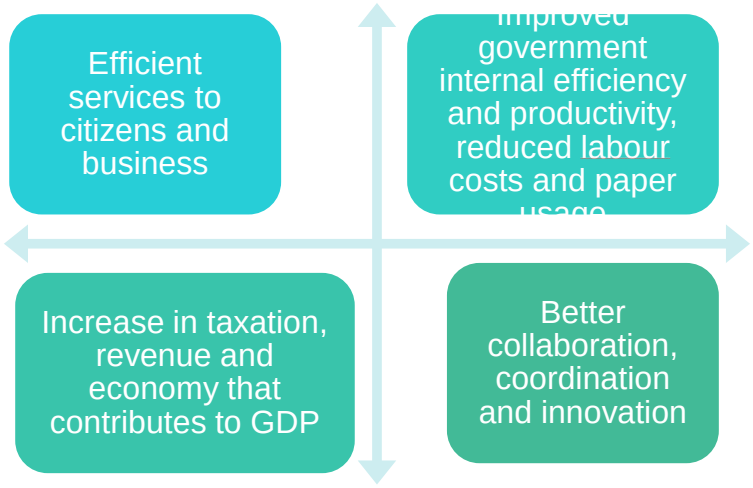

Figure 4: Benefits of Digital Government

Enhanced digital delivery of government services could bring financial benefits to governments through improved efficiency and cost savings in areas such as time savings, shared digital resources between agencies, and reduced storage costs through cloud technology. Digitalisation can also improve operating efficiency across and within agencies by leveraging shared platforms and resources. Citizens or visitors can access digital public services that are simple, secure, and available anytime, anywhere. Enterprises will find registering and operating a business easier, simpler, and faster. A faster and more efficient service reduces the burden of business and citizens visiting different government offices, saving time and hassle. The digital government also

[4] Corsi, M., Gumina, A., & D'Ippoliti, C. 2006. eGovernment Economics Project (eGEP): Economic model-final version. Nr., eGovernment Unit, DG Information Society and Media, European Commission, Brussels.

increases transparency, making it easier to track corrupt practices, thus fostering trust between the government and citizens.

Digital government is also essential for growing the digital enterprise ecosystem, positively contributing to economic growth by enabling them to create innovative services and products. The government has significant procurement potential in digital technologies, which can support the development of small and medium enterprises. Overall, a well-developed digital public service enhances the national profile, drives confidence and investment and creates a better quality of life for its citizens, businesses, other residents and visitors.

2.2 Drivers for Digital Government

Technological advancements, geopolitical shifts, the economic environment, emergencies like the COVID-19 pandemic, and disasters are transforming the adoption of digital technologies across the government. COVID-19 has made the necessity of digitalisation and a digital government even more urgent. The growing users' expectation to access faster and more efficient services, increasing use of disruptive technologies, and growing experience delivering shared digital government have also spurred technology integration in public services. On the negative side, the digital government can exacerbate the digital divide and lead to cyber threat issues that must be managed.

At the heart of government digital transformation is the increasing generation and use of data. The availability of cheaper storage and processing power, the increasing availability of data via online social networks and the Internet of Things (IoT), and improvements in data analytics delivered through 'deep learning' have made data central to digital public service. Modern Artificial Intelligence (AI) extracts value from data and more data availability results in more accurate AI models. This, in turn, means greater potential benefits to government, society and business.

Box I: Positive and Negative Drivers of Digital Government

Positive Drivers

- Users' expectations are growing- the increasing use of social media and the Internet has led to a tech-savvy population that demands better and more efficient services. Governments worldwide are rapidly changing how they engage with people to deliver modern digital services to meet users' expectations.
- Advances in processing power and storage are making it easier- the availability of modern, efficient data infrastructure (data centres, cloud computing and content delivery networks) has made it easier for the government to collect, analyse and provide massive amounts of data.
- Disruptive technologies are stimulating digital government – emerging and disruptive technologies such as artificial intelligence, cloud computing, connected devices, and robotics are rapidly reshaping business, communication and delivery of services. At the same time, privacy, safety and stability issues demand smart policy and strategic responses that can keep pace and evolve with technology.

- Digital technologies are essential to drive jobs in public and private sectors - demand for technology workers in the public sector is rising, further impacting the digital skills shortage.

Negative Drivers

- Digital public services can increase cyber threat - the dependence on digital technology exposes vulnerabilities that threaten the safety of individuals, communities and businesses and must be met with extensive, intelligent safeguards and improved digital literacy.
- Digital public services pose the challenge of digital inclusion because people who don't have access to technology or digital skills risk being left behind. Despite current improvements, a substantial portion of the population do not have access to the internet or digital connectivity, and most households do not have the necessary tools like power, computers and smartphones to access digital government services.

2.3 Best Practices, Lessons Learned from Other Countries' Digital Government Strategies

Digital government has been progressing across the world. Therefore, there is a lot to learn from every nation. A review of best practices worldwide in general and experiences of Australia, Brazil, Canada, Estonia, India, Kenya, Korea, Rwanda, South Africa, Tunisia and Zambia that were surveyed for this assignment, in particular, indicates that successful governments have made considerable progress in formulating digital government policies and legal frameworks, building and improving digital infrastructure, strengthening digital government services, supporting capacity building, promoting the partnership between government and the private sector, and making funding available for digital public services. They have also been reforming government processes and ensuring services are designed around citizens' needs and key life events.

Governments have also been fostering a data and insights-driven culture by consolidating data from government silos, thus making quality, open data more accessible to drive and support their decisions and to promote private sector innovations. Almost all countries have[5] adopted an omnichannel approach to service delivery. Public services are provided through a national web portal and mobile applications, which provide a one-stop window for citizens and businesses to obtain information, easily interact with the government, and make secure payment transactions at all places and times.

[5] Countries covered in the assessment include Australia, Brazil, Estonia, India, Kenya, Korea, Rwanda, South Africa, Tunisia and Zambia, UK, USA, Canada, New Zealand, Ireland, Kiribati, Papua New Guinea, Uganda, Tanzania, Nigeria, Kingdom of Saudi Arabia, Mauritius, Taiwan, Lebanon, Switzerland, Bahrain, Mexico, Uruguay, Vietnam, Germany, UAE, Qatar, the Netherlands, Indonesia Afghanistan, Morocco, Malawi, Montenegro, Trinidad and Tobago and Uzbekistan.

Countries with a high level of digital government development focus on strengthening their leadership and digital skills, as well as building digital literacy of all stakeholders - civil servants, regional and local governments, students and citizens, paying attention to research, development and innovation, and using the latest advanced technologies, such as big data, artificial intelligence, blockchain, cloud technology, and Internet of Things. Integrating digital literacy programs into public and private education systems is also considered a national digital development agenda in other countries. This was achieved through the modernization of the education system's infrastructure, the provision of incentives for teachers and leaders of educational institutions, the change to digital teaching methods, and the embracing of coding and digital culture in teaching and learning.

A significant effort has also been made to advance the digital ecosystem, especially in promoting public and private partnerships. Governments and the private sector have been working together to invest in digital infrastructure and set up ecosystems to support digital government services, including maintenance, training, research, development, and innovation. Examples include Lithuania[6] and Luxemburg[7], where the government established GovTech Labs, which are intended to bring digital government challenges to the private sector's innovations. In some countries, for example, partnership mechanisms between public and private sectors have spurred investment in developing network infrastructure and data centres on a " invest first, pay later" basis.

Funding was also the main issue that countries have addressed—funding sources from the national budget, private sector, development partners, and other sources, such as the use of universal service funds, have been explored by different countries. In advanced countries, for example, a major funding source is an annual budget determined by the government at a rate of the GDP for digital public service. Successful countries do not only allocate funding but also measure progress against initiatives and define key performance indicators.

Digital government skills have been a key challenge for most governments. Governments have encouraged upskilling whilst recognising the missing digital talent and identifying ways to fill these gaps. Coordination has also been an issue across countries, but successful digital governments began by ensuring the governance framework was right. Some techniques for good digital governance include establishing a digital government coordinating institution closer to the highest decision-making, establishing a dynamic digital government support centre and ensuring everyone is consulted on digital government issues at national and sub-national levels.

Further, the experiences of the countries suggest the need for:

- Building the necessary digital government infrastructure– country experiences show that the building and improvement of digital government infrastructure

[6] https://govtechlab.lt/

[7] https://govtechlab.public.lu/en.html

must focus on quality and scope, including the building of high-speed Internet infrastructure, national, regional and district government connectivity, data centres, data exchange platforms, payment gateways, digital identity infrastructure, digital authentication infrastructure and digital security infrastructure.

- Integrating emerging technologies in digital public services. Advanced digital government countries like Korea and Singapore have invested in emerging technologies such as artificial intelligence, the Internet of Things, blockchain, cloud and predictive analytics to improve government decision-making, service design and delivery.
- Increased focus and investment in cybersecurity are needed to ensure safe and secure systems and build citizens' confidence in their data privacy and security.

Table 2: Summary of Lessons from Selected Countries

E-Government Theme	Best Practice
Technology Infrastructure and services	**Zambia** has developed a common Government Wide Area Network (GWAN) that provides shared network services and Internet to all Ministerial headquarters and provincial offices. **Zambia** has also established ZamConnect Enterprise Service Bus based on Estonia's X-Road **Estonia** invested in open-source solutions as foundation of digital government. **Estonia** has strong digital identification of citizens, a digital data exchange layer (X-road) and diverse applications developed by different public and private institutions. **Korea** promotes applications reuse through an eGovernment Standard Framework (eGovFrame). The Government of **Kenya** has built approximately 9000km of terrestrial fibre that has reached sub-county levels, mainly connecting key government institutions. The Government of **Kenya** has established the National Data Centre at Konza Technopolis, a cloud-based, tier 3 data Centre set that plays a key role in the digital government agenda.
Financing	**Kenya's** dedicated budget aims to provide universal access to eGovernment services.
Public administration reform and change management	In 2022, **Australia** completed a review of digital capability across twenty agencies responsible for most of the Government's digital services. The results were used to improve digital government services reform by upskilling public servants, including senior leaders. In **Mauritius**, each ministry submits an annual mandatory ICT report to the Ministry (MTCI) on the development of the ICT, the performance of public operators on the quality of service, and consumer satisfaction, among others.
User-centred design -	The **Australian** Government conducts surveys to identify users' challenges when using e-services.

	South Africa pays attention to user-centricity and the diverse languages of the population in its eGovernment development. The **Tunisian** government promotes eGovernment services through government portals using citizens' digital identities as an authentication tool. In **India**, the e-District project has been implemented at district and sub-district levels of all States, benefitting all citizens by delivering various eServices such as Certificates (Birth, Caste, Death, Income, Pension (Old Age, Disability and Widow), Electoral, Consumer Court, Revenue Court, Land Record and services of various departments such as Commercial Tax, Agriculture, Labour, Employment Training and Skill Development etc.
Leadership and Governance	**Korea** created a Government Reforms Committee in the 2000s, which reports directly to the President. In **Estonia**, eGovernment is led by the office of the Deputy Secretary General for Digital Development (Ministry of Economic Affairs) In **Australia**, the move of the DTA to the central Prime Minister and Cabinet portfolio in April 2021 strengthened its mandate and placed concentrated attention on digital Strategy investment and assurance across the Australian Public Services. The Electronic Government Act 2021 of **Zambia** aims to enhance the management and promotion of electronic government services and processes and establish the Electronic Government Division in the Office of the President.
Digital ecosystem development	**Rwanda** has attracted a series of centres of excellence, including the African Institute for Mathematical Sciences (AIMS), which is now based in Kigali, the Carnegie Mellon University- Africa, the African Centre of Excellence in IoT and the African Centre of Excellence on Data Science. The new Digital and Future Skills Strategy8 of **South Africa** discusses initiatives intended to contribute to the capacities of South Africans to meet the challenges arising from the increasing deployment and adoption of emerging technologies like cloud technologies, big data analytics, artificial intelligence, virtual and augmented reality, autonomous vehicles and drones, Internet of Things, robotics and 3D printing.
Legislations and regulations	**Australia** established regulatory frameworks supporting eGovernment covering personal data protection. Brazil mandates government institutions to increase the availability of public services in digital and online formats by legislating digital by default principle and ensuring online services within a specified time frame.
Security, privacy and resilience	CybExer Technologies, an **Estonian** cybersecurity company, provides highly sophisticated cybersecurity training platforms with a special focus on cyber capability development. **Mauritius** has developed a National Cyber Security Strategy 2014-2019, which provides an overview of what it takes to protect information systems and networks effectively and gives an insight into the Government's approach and Strategy for protecting cyberspace. It has also developed a National

[8] https://www.gov.za/documents/national-integrated-ict-policy-white-paper-national-digital-and-future-skills-strategy

	Cybercrime Strategy 2017-2019 to enhance the law enforcement's capacity and strengthen the legal framework to combat cybercrime effectively.
Data infrastructure	The **Australian** Data and Digital Government Strategy aims to use data and digital technologies to improve government activities, including the delivery of services. **Brazil** is at the forefront of making open data available for citizens, researchers and businesses. It has adopted an Open Data Policy and implemented an Open Data Portal - a centralised form for accessing government open data. India's Open Government Data platform has over 610,000 resources and 13,000 catalogues, with 9 million downloads by 2023.
Emerging technology integration	**Korea's** Digital Government strategy integrates emerging technologies, the Internet of Things (IoT), cloud computing, big data analytics, mobile devices, and other intelligent technologies

3 An Assessment of the Current State of Digital Government in Ethiopia

3.1 Digital Government Situation Assessment Methodology

The development of this digital government strategy follows extensive consultation with the public and the private sector, as well as a review of the achievement of the eGovernment strategy of 2011-2015 and the eGovernment Strategic Plan of 2016-2020. The assessment adopted a user-centric approach to ensure that the digital government responds to citizens' and businesses' requirements.

The development process for the Digital Government Strategy included reviewing key documents, consulting with stakeholders, analysing the situation of eGovernment services within Ministries, Departments, Agencies and regional governments, reviewing international practices and analysing the overall digital government evolution gap.

- Document analysis covered core overarching policies, plans, legislations and digital government programmes in Ethiopia. These included the Homegrown Economic Reform agenda, the 10-Year National Prosperity Development Plan and Digital Ethiopia 2025. The government also drafted a national ICT policy in 2016, which was not adopted. In the eGovernment area, the GoE has adopted two five-year e-government strategies (the first from 2011- 2015 and the second from 2016-2020). Efforts were also made to adopt eGovernment Enterprise Architecture in 2011, which was revised in 2019. Other supporting policies, programmes, legislations, and strategies reviewed include the National Digital Payments Strategy, Electronic Transaction Proclamation, Computer Crime Proclamation, Communications Service Proclamation, National Financial Inclusion Strategy, and the National Digital ID Program. An extensive review of a national digital health strategy and blueprint was also made, along with documents produced by partners such as the Tony Blair Institute and GIZ-implemented Business Environment and Investment Climate, including the eGovernment project. The review was intended to understand the Political, Economic, Social, Technological and Legal (PESTL) environment of digital government in Ethiopia.
- The Voice of Customer survey was conducted between March and November 2023 and covered 350 individuals. Initial data were collected from the Oromia, Amhara, SNNP, Somali, and Sidama regions, where most respondents were located. This was followed by a collection in Addis Ababa and Dire Dawa, as well as the other

remaining regions, namely Harari, Afar, South West Ethiopia, Gambelia, Benishangul, and Tigray.

- The stakeholders' consultation involved semi-structured interviews with central and local government, the private sector and civil society organisations. The consultation took place between February and August 2023. It covered over 150 individuals from the federal and regional governments. The private sector, academia, and civil society organisations were also included, but the consultation with these groups was minimal due to time limitations. The consulting team interacted with more than eleven ministries, ten agencies, one university and three private sector entities. In parallel with this process, the team conducted bilateral conversations with key partners, including the GIZ-implemented Business Environment and Investment Climate, the eGovernment (BEIC) Project and the Tony Blair Institute.
- The situation assessment focused on mapping the digital technology environments and eServices situation in 32 MDAs that participated in the survey based on the E-Government Development Index (EGDI) themes: institutional framework, technical infrastructure, service provision, content provision and e-participation.
- The International best practices assessed the experiences of many countries with successful digital government initiatives. Specific attention was given to:
    - Experiences of countries at the top of EGDI and GTMI – Australia, Estonia and Korea,
    - Experience of African Countries that have successfully implemented eGovernment services and rank high on EGDI and GTMI - Mauritius, Rwanda, Kenya, South Africa, Tunisia and Zambia,
    - Experience of countries in the global south that have large population sizes, multiple local language challenges, the political and economy of decentralised administration like that of Ethiopia and which at the same time successfully developed exemplary digital government services – Brazil and India. The report also presents the experiences of the European Union in coordinating the Interoperable Europe Initiative[9] aimed at cross-border digital public services to draw lessons related to the connected government approach with regional cooperation at the core.
- Finally, an overall gap analysis was carried out to present the state of digital government using the World Bank's Digital Government Readiness Assessment themes – namely – (i) leadership, coordination, governance, (ii) digital skills, (iii) user-centred e-services and channels, (iv) Infrastructure, (v)legislation and regulation, (vi)data, data strategies and governance (vii) cybersecurity, privacy and resilience (viii) public administration reform and change management and (ix) supporting digital ecosystem.

[9] https://joinup.ec.europa.eu/interoperable-europe

The data were then used to define the digital government strategy's vision, mission, theme and objectives and outline the foundations and enablers for delivering public services over the coming five years.

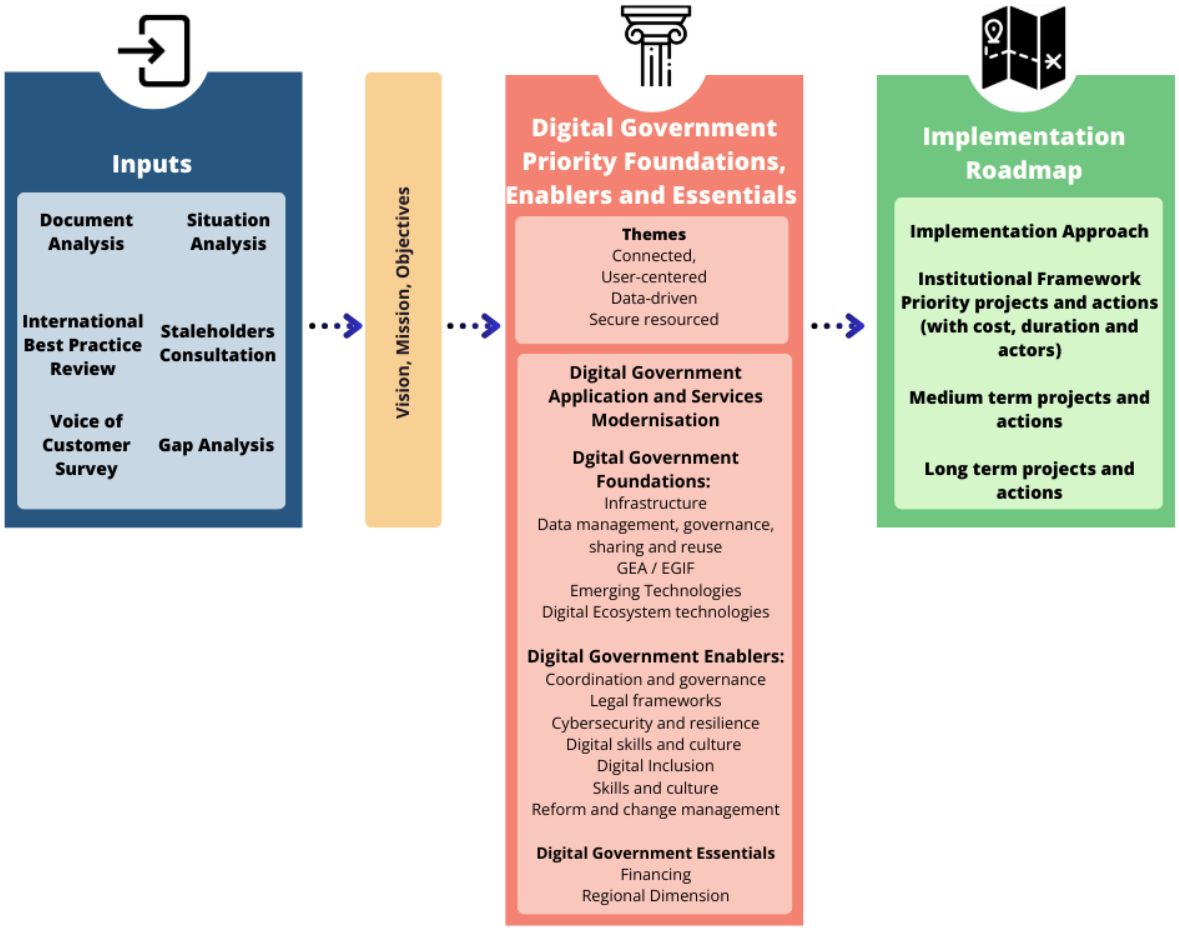

Figure 5: Methodology for Design of Digital Government Strategy

While efforts were made to reach out to as many stakeholders as possible, meeting with all ministries, departments, agencies, and regional and local entities in the government was difficult. The recommendations of the Digital Government Strategy are based on the assessment study of 32 MDAs that participated in the analysis between February and August 2023. Thus, the information presented in the strategy is based on the inputs received through questionnaires and interactions with the Ministries, Departments and Agencies. No separate field validation study has been conducted on the data received from ministries/agencies.

3.2 Digital Government Baseline

Ethiopia's progress in digital government is symptomatic of its social and economic development challenges. Low digital infrastructure development, educational attainment, and limited transactional services suggest Ethiopia's global standing in digital public services remains very low. Baseline data presented in Table 3 indicates that a few

institutions provide online public services for a relatively low percentage of the population that uses the Internet.

Table 3: Baseline Data of Digital Government in Ethiopia

No	E-Government	Data for 2023/2024
1	Number of eGovernment services on https://www.eservices.gov.et/	750
2	Number of visitors	3,112,387
3	Number of processed applications via https://www.eservices.gov.et/	574,200
4	Number of public institutions providing e-Services on national portal	25
5	Percentage of the population that has some contact with digital government services	4%
6	E-Government Development Index	0.3111
7	E-Government Development Index ranking	169/193
8	UN E-participation Index	0.1644
9	GovTech Maturity Index	0.58
10	Global Cybersecurity Index Score	76.34%
11	Internet penetration	39.3%
12	Mobile penetration	72%

3.3 Digital Government Status

The situation analysis indicates that the Government of Ethiopia has made strides in digitalising public services over the last two decades. In addition to increasing the use of computers and the Internet in the public sector, the GoE has invested in several digitalisation projects, namely WoredaNet, which connects districts to central government; SchoolNet and EthERNet, which links schools, colleges and universities to modern applications and services, respectively National Data Centre, e-Services Portal, and a multitude of sector-specific information systems including Integrated Financial Management System (IFMIS), SIGTAS which is used for the digitalisation of tax filing and collection processes, digital ID systems and electronic voting system.

The situation analysis that drew on the Digital Government Readiness Assessment (DGRA) framework shows that, despite progress, there have been challenges with non-interoperable service delivery, uncoordinated business processes, inadequate data centre and Internet infrastructure, and low levels of ICT knowledge and skills in the public sector. The following section provides highlights of the findings:

User-Centred services—The Government of Ethiopia intends to make 2500 eServices available to citizens and businesses. However, there is a lack of prioritisation of the services based on citizens' and business needs. The other issues that need to be addressed concerning eServices are as follows:

- Current eServices are largely informational.
- Transactional services are still in their infancy,
- Current eServices are not designed based on users' and businesses' end-to-end journeys.
- While digital and mobile payment integration has improved, there still needs to be more mobile applications.
- User-centred eServices principles and standards are not considered in eService design.
- Most eServices are not designed based on business process transformation; thus, there is a tendency to automate inefficient services.
- The limited progress with digital Identity means a few users could use transactional services.

Governance and coordination—Ethiopia's digital public service governance framework remains weak. While the MInT provides overall guidance for digital government, the responsibilities of digital government support institutions like the AI Institute, INSA, MInT and the Digital Transformation Council overlap. Recently, the Governance has improved following the establishment of the Digital Transformation Council. The MInT lacks the necessary staff with state-of-the-art digital technology skills to coordinate the delivery of digital services.

Digital Skills and Culture—Another concern is the low level of digital skills at MDAs and regional governments. Most institutions indicated that they could not attract and retain digital talent due to low remuneration and limited incentives in the public sector.

Financing—Funding digital services is another issue that made it difficult for most MDAs to extend their online services. There is a significant dependence on donor funding; thus, resources available through the public budget are limited. The limited cost-saving strategy, low adherence to standards, and long duration for purchase and implementation of digital government infrastructure and services all add up to the challenges to effective financing eServices.

Infrastructure and Interoperability—The limited capacity to implement government-wide enterprise architecture and interoperability framework and lack of skills in this area means digital technologies are implemented without coordination at application, services, data and business process levels. An Enterprise Service Bus (ESB) that connects all applications has not been implemented. Shared infrastructure like the data centre and WoredaNet have reliability and capacity issues. Most MDAs operate low bandwidth networks, making it difficult to serve citizens and businesses.

Data Management, Use and Sharing—The Government of Ethiopia has initiated a data management, sharing and use programme, but efforts to date remain inadequate. Efforts

are underway to develop personal, business and land registries. Still, much must be done to increase the scope and quality of this core data and begin sharing and reusing it based on well-designed data governance and specifications. Data quality is inconsistent and poor, and effective data sharing between departments is limited. The GoE is not proactively publishing open datasets and encouraging their use.

Legislations—Ethiopia adopted key legislation concerning electronic transactions, cybercrime, digital signatures, and data protection, which need additional guidelines. Other legislative areas that need improvement include the once-only principle, digital-by-default principle and security-by-design principle. Policies, strategies, and legislation concerning emerging technologies – e.g., IoT, blockchain, AI, cloud computing, and green IT use in government- are also desired.

Cybersecurity and Business Continuity—The growing cyber threat necessitates that the government step up its security infrastructure and develop strategies and plans for cybersecurity and critical information infrastructure. Advanced cybersecurity skills and the population's and civil servants' awareness of impending cyber threats when using digital services must also be improved.

Digital Government Ecosystem—Ethiopia's digital economy ecosystem, comprising entrepreneurs and research institutions, is less developed than other countries. A significant effort is still needed to promote the startups through hubs, incubators, and accelerators, as well as reform the academic curriculum to gear it towards solving digital government problems. Finally, the regional dimension needs integration, including policy, regulatory and legislative harmonisation, to ensure the flow of goods, services and experts across African borders within the African Continental Free Trade Area framework. International partnerships are key to increasing the benefits of digital technologies and reducing transnational harms, such as cybersecurity and information disorder.

3.4 Strengths, Weakness, Opportunities and Threats of Digital Government

Table 4 summarises the identified strengths, weaknesses, opportunities and threats of digital government based on international practice and internal situation assessment.

Table 4: Strengths, Weaknesses, Opportunities and Threats

Strength	Weaknesses
The government has the political will and support of digital government per the rapid technological advancement and needs of citizens and business The Ministry of Innovation and Technology leads and coordinates the implementation of the digital Ethiopia Strategy. The MInT is committed to coordinating and implementing	In 2024, Ethiopia was ranked 169th out of 193 countries according to the UN-DESA assessment on infrastructure, online services, and human capital. In that, the online services and human capital indexes ranked low compared to the average ranking in Africa. Digital government policies and action plans have not been fully implemented due to various reasons,

successful digital government policies, applications and services. Relevant ministries and institutions are highly committed to cooperate on the implementation of digital government services. Strong digital foundations are in place. Ethiotelecom has laid around 22 000 kilometers of backbone optical fiber and more than 13.3K kilometers of metro optical fiber network, in addition to modern hosting infrasture. Its international internet gateway has reached 1.82Tbs (1.09 IGW and 742Gbs Cache for google, meta and Netflix).	especially the limited budget and continuous reorganization of MDAs. Some ministries and institutions have not yet set up a well-staffed unit in charge of digital transformation with clear roles and responsibilities that can work effectively. Ministries and institutions set up digital information systems according to their needs and in isolation, without consistency or overlap. Telecommunication infrastructure does not cover the whole country yet. The network connection between ministries, institutions, regional, zonal, district and local administrations is insufficient The national data centre remains inefficient regarding computing power, storage and connection to MDAs. National platforms and common systems for sharing, using, and exchanging data remain insufficient. A common digital identity infrastructure that is a lever to encourage online transactions is still under development. Digital security protection in ministries and institutions is still low. Ministries and institutions have almost no digital security infrastructure, use software without security standards or proper licenses, and lack the technical capacity to monitor, analyse, control, prevent, and respond to cyber-attacks. The eServices have not been fully integrated with national payment and mobile gateway; thus, a few government entities provide end-to-end services. The number and capacity of human resources with digital technology skills in MDAs and regional governments are still limited, a major obstacle to developing, managing, operating, and maintaining digital government systems. Ethiopia's entrepreneurship and academic ecosystem is underdeveloped. The ecosystem is inadequate to support public and private sector partnerships and does not have the momentum to drive innovation.
Opportunities	**Threats**

Digital technologies promise significant benefits for the citizens and businesses that expect improvement in public services and the connection between government and the people. The spread of COVID-19 has caused the importance of the use of digital technology in administration, business, and social networks. Internet and social media usage is growing. The government can use this growing Internet and social media to deliver digital services. Ethiopia can adopt the latest technologies and tools and digital public goods than investing in legacy systems Emerging technologies like artificial intelligence, big data, blockchain, cloud technology, and the Internet of Things can be leveraged to deliver better digital public services. There is a growing regional and international consensus, technical knowledge and support for digital government services that Ethiopia can tap into.	There is a growing cyber threat for digital government. Geopolitical conflicts and cyber warfare can undermine the development of networks, digital economy integration, and digitalisation of public services. Large-scale natural disasters have a long-term impact on digital connectivity infrastructure, such as submarine fibre-optic cable networks, backbone fibre-optic cable networks, and data centres. Outbreaks of epidemics, regional and global financial crises, and the collapse of technology companies can affect the development of digital government.

Part II: Vision, Objectives, Guiding Principles, and Prioritized Interventions

4 Vision, Mission and Strategic Objectives of Digital Government

This Digital Government Strategy ensures citizens and businesses are at the centre of the transformed government's service delivery. By ensuring users' needs and convenience at the core, this Strategy aims to ensure integrated, secure, effective, transparent, and efficient end-to-end digital public services. The strategy proposes that digital services be accessible over the Internet through mobile phones, digital TV, call centres, and personal computers. It is based on a digital-first principle; thus, all public-facing services must be developed to be available regardless of social and economic status, disability, gender and other factors that the users may experience.

4.1 Vision

A connected, user-centric, data-driven, secure, sustainable and digitally transformed government providing affordable and efficient service to all.

4.2 Mission

The mission of the digital government strategy is to:

- Accelerate a whole-of-government approach by sharing and reusing applications, services and infrastructure to improve the quality and efficiency of public service delivery.
- Deliver user-centred, data-driven, secure, transparent services to citizens, businesses, visitors and government.
- Maximise the value of data for decision-making, economic value creation and innovation.
- Ensure the use of digital technologies contributes to a sustainable environment and ecosystem.
- To support the digital transformation of government, promote digital literacy, skills, research, innovation, digital services culture and entrepreneurship.
- Leverage emerging technologies for efficient and quality public service delivery.

4.3 Objectives

The strategic objectives of the digital government are to:

i. Provide integrated, easy, fast and accessible applications and services that are designed based on the needs of citizens, businesses, visitors and civil service, considering their journey and life events. Ensure 80% of user services are available online by 2030.

ii. Provide a world-class digital infrastructure for connected government: Ensure 80% of central and regional government entities are connected to an IP-based Government Wide Area Network and National Data Centre by 2030
iii. Ensure better coordination and governance of digital public services: By 2028, fully adopt GovStack to achieve a seamless digital government.
iv. Raise the level of digital capabilities and skills for the government ICT workforce, civil servants and the public: By 2030, 50% of the government ICT workforce will be trained, with at least 5% receiving different certifications.
v. Ensure legislation readiness for smooth and comprehensive digital transformation: Adopt legislation by 2030 that promotes emerging technologies and mitigates their risks.
vi. Facilitate a whole-of-government approach through interoperability and shared applications and services: connect all government entities to Ethio-connect enterprise service bus by 2027.
vii. Ensure emerging technologies are integrated into digital public services to enhance transparency and decision-making. By 2030, ensure that at least a quarter of public applications and services are built in emerging technologies like AI, blockchain, IoT and data analytics.
viii. Expand the digital ecosystem of innovation, research and entrepreneurship in support of government transformation. By 2029, ensure that 30% of digital government solutions are developed by local entrepreneurs.
ix. Facilitate digital inclusion to ensure that no one is left behind in the use of digital public services ––explore satellite internet connectivity possibilities for accelerating national broadband coverage to 100%.
x. Ensure the resilience and security of digital public services by ensuring that 50% of public entities are certified for zero-trust security by INSA by 2030.
xi. Facilitate administration, process reform, and change management for government digital transformation. Ensure that 80% of digital services are accompanied by business process reform and service redesign.
xii. Accelerate regional and global digital integration to improve data flow for cross-border trade of goods and services- play leadership role in at least 20 % regional digital and emerging technology strategies, policies and frameworks.

The end state of digital government is to achieve a fully digitalised user-centred, secured paperless government that improves public services delivery and increases transparency and accountability.

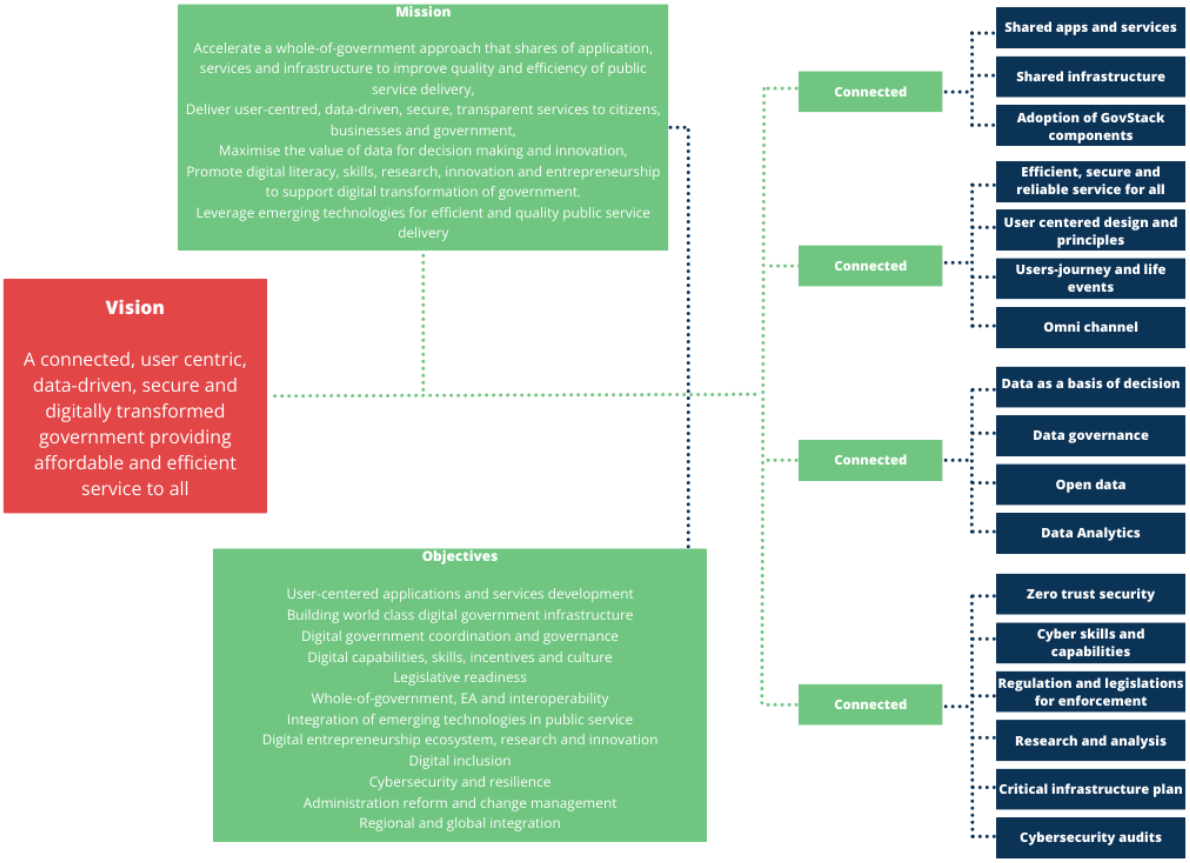

Figure 6: Relationship between Mission, Vision, Objectives and Digital Government Themes

The above objectives indicate that digital government needs to focus not only on the modernisation of technology, services and data but also on re-examining public service processes and, more importantly, developing people's capacities and their engagement with eServices. Ethiopia will shift towards the "people" aspect (skills, inclusion, culture) of digital government while leveraging digital and emerging technologies and data to deliver efficient public service.

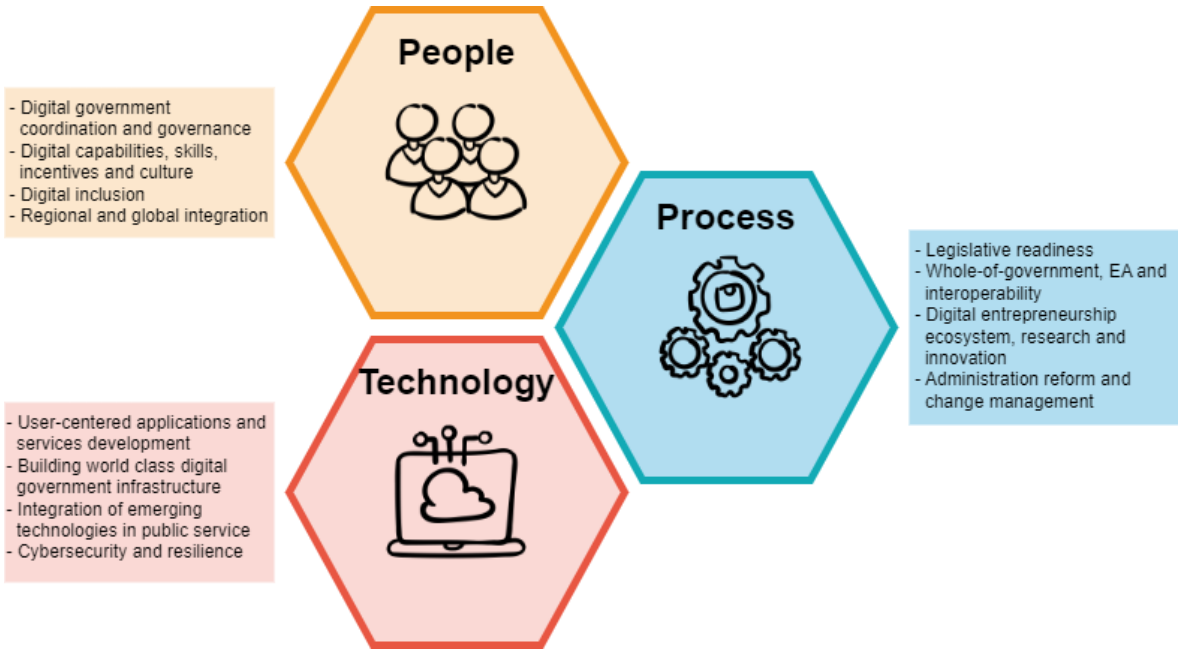

Figure 7: Technology, People and Engagement and Process Dimensions of Digital Government

4.4 Digital Government Themes

The Digital Government Strategy 2025-2030 will strive to achieve a user-centred, data-driven, secure and environmentally sustainable whole of government with attention to delivering end-to-end shared digital public service. The Strategic Themes were selected to ensure that GoE transitions from an "eGovernment" stage, where the government remains a provider with one-way communication, to a "digital government" stage emphasising use-driven public service, where procedures are digital-by-design, data-driven and environmentally sustainable. Therefore, Ethiopia will build:

- A Connected Government in which:
    - future digital solutions focus on the reuse of data, shared architecture and standards that enable integration across government applications and services,
    - shared infrastructure is built, including data centre and cloud services and state of the art broadband network (GWAN) to connect federal, regional and local government entities across the country,
    - the government adopts the GovStack building block approach to create reusable components, gradually build interconnected services, and advance towards a cutting-edge GovTech environment.
- User-centred government in which:
    - the government provides useful and impactful services to citizens, businesses and civil servants,
    - government ensures citizens, businesses and civil servants have accessible, efficient, secure and reliable services that are higher quality and more personalised, proactive and inclusive services, taking language, economic, geographic, gender, culture and other diversities into consideration,

    - a user-centric methodology is used to design, develop and integrate services, catering to the requirements of citizens, businesses, government employees and visitors,
    - systems are designed based on users' needs, life events and journeys and draw on user-centred design principles and
    - an omnichannel service strategy for citizens is adopted to promote a homogeneous, inclusive, high-quality experience.
- Data-driven government in which:
    - data are collected, organised and shared to improve service delivery, support more-informed decisions, bring greater rigour to policy and program evaluation, and drive private sector innovation.
    - the government governs data as a key strategic asset in generating public value by applying it in planning, delivering and monitoring public policies and adopting rules and ethical principles for their trustworthy and safe reuse.
    - the government ensures data that does not have personally identifiable information is available online to facilitate citizens' and businesses' access to open data for engagement, innovation and generating the private sector's economic value and
    - capacity in research and analytics is built to use massive data available from the public and private sectors to drive social and economic development.
    - The government promotes open standards and access to public data, as well as to facilitate the interoperability of government information systems.
- A secure government where:
    - zero trust security is maintained at every level of government, and plans are in place to identify, protect, detect, respond and quickly recover from cyber threats,
    - skills and capacities are built at every level of government to detect, respond, and recover from cyber threats,
    - regulatory framework and the development of capacities for persecution and prosecution of crimes,
    - research and analysis are conducted on an ongoing basis to fight cybercrime,
    - a national critical infrastructure plan that defines minimum cybersecurity requirements for the critical information assets developed to mitigate cyber risks,
    - ongoing audits are conducted towards adoption and compliance with government cybersecurity strategy and standards.
- An environmentally sustainable government in which the government, which
    - encourages the development and use of digital and emerging technologies with sustainability considerations. This includes the use of long-lasting and green (energy star) technologies, reducing energy consumption, promoting

eco-friendly practices in digital government operations and reducing electronic waste (e-waste) through appropriate recycling,

- promotes innovation-driven ecosystem rather than adopting closed "off-the-shelf" solutions, which lead to dependency,
- provides appropriate guidelines for Environmental, Social and Governance (ESG) consideration in the use of digital technologies for public administration,

4.5 Principles

The Digital Government will be interoperable, connected and integrated, with citizen-centric services at its core. Table 5 outlines the core principles of connected, user-centric and data-driven digital government, which underscores digital government 2025-2030.

Table 5: Principles of Digital Government

Once-Only Principle – Ministries, departments, agencies, and regional and local governments will ensure that citizens and businesses only supply the same information to public administrations once. This will reduce the entry of inconsistent data, administrative costs, and the workload of government and stakeholders in collecting, storing, and using data. Data collected at the source will be shared and reused between public institutions.	**Data-Driven Culture –** data will be a key strategic asset in generating public value through its application in the planning, delivery, and monitoring public policies. The government will collect, manage, and integrate public data to drive innovation, value creation, informed decision-making, policy formulation, monitoring, and continuous improvement of the quality of services.
Digital-by-Default /Digital First– All public institutions will provide services via the digital channel by default while assisting users with limited digital skills in using digital services via support desks.	**Cloud-First** – the GoE, will adopt cloud technologies for all new applications, platforms and infrastructures.
Open by default – all government data not containing personally identifiable information will be available on the open data platform. MDAs will release non-personal and non-sensitive data of public interest in an open and anonymised format.	**Open Standards and Open Platforms** -an open approach **adoption of cloud technologies for all new applications, platforms and infrastructure**collaboration and avoid duplicating work already done as much as possible; digital government services will be developed based on open platforms and standards.
Interoperability as an ecosystem - all government digital information systems will operate independently and link with each other through legal, organizational, semantic and technical interoperability. MDAs regional and local government will adhere to the Government Enterprise Architecture and Interoperability Framework to attain user-driven, consistent, seamless, integrated**,**	**Privacy by Design** – The privacy of citizens will be protected during digital transactions. Measures will be taken to minimize collection and protect confidential information and the identities of individuals in data sets from unauthorized access and manipulation by third parties.

proactive, and cross-sectoral services.	
Design with the user in mind – all systems will be designed through the involvement of citizens and other stakeholders in the conception and design of services. Citizens and businesses will indicate and communicate their own needs and, thereby, drive the design of digital public services.	**Security by Design** – digital applications and services will be designed, developed, and operated to be resilient to cyber threats to protect citizens, businesses, and government data.
End-to-end Services – all eServices will be transformed into transactional services with end-to-end paperless services that do not require physical travel or office hopping through cross-agency collaboration, interoperability and data sharing between systems.	**Multi-channel delivery -** different channels for service delivery will be implemented to offer access to services for all citizens and businesses without needing specific service delivery channels and tools.
Digital Inclusiveness and E-Participation – Digital services will be built to address better the specific context, culture, behaviours and expectations of citizens and businesses, including people at the margins like women, rural people and those with disabilities. The needs of different social groups of the population will be considered when developing digital services – e.g., people with limited access, people with disabilities, etc. Digital platforms will gather citizens' and other stakeholders' views and act on them in government decision-making processes.	**Open innovation -** Digital public services will be developed with open innovation, digital public goods and digital public infrastructure at the heart to ensure the reuse and sharing of data and applications. The GoE will adopt the GovStack building blocks, digital public goods, and digital public infrastructure framework to drive innovation, sharing, and reuse of applications.

4.6 Strategic Alignment of Digital Government

This Digital Government Strategy is aligned with the 2019 Homegrown Economic Reform Agenda, the Ten-Year Development Plan (2020-2030), and Digital Ethiopia 2030, as well as with international commitments such as the Sustainable Development Goals, the African Union Digital Transformation Strategy, the African Data Policy Framework and its Convention on Cybersecurity and Personal Data Protection. The legislative mandates of the strategy are covered in the following laws: Negarit Gazette of the Federal Democratic Republic of Ethiopia Proclamation No.1263/2021, Communications Service Proclamation No. 1148/2019, Electronic Transaction Proclamation No. 1205/2020, Electronic Signature Proclamation No. 1072/2018 and the Personal Data Protection Proclamation (No. 1321/2024).

4.6.1 Alignment with the National Development Plans

The Digital Government Strategy is guided by and aligned with the Homegrown Economic Reform (HGER 2.0), Ten Year Development Plan (TYDP) and Digital Ethiopia 2025. HGER

2.0 and TYDP emphasise the critical importance of digital financial services and establishing a digital economy focusing on agriculture, manufacturing, and service sectors. HGER 2.0 and TYDP accentuate digital platforms for tax collection, financial inclusion, improving public finance management, adopting eGovernment services, enhancing digital public records management, and online platforms for citizen engagement. To integrate digital technologies in the public sector, HGER and TYDP recommend improving access to data infrastructure, developing skills, maintaining cybersecurity, and enhancing digital entrepreneurship.

Digital Ethiopia 2025 is important because it identifies four main pathways for development:

i. Unleashing value from agriculture.
ii. Future global value chains in manufacturing.
iii. Building IT-enabled services; and
iv. Digital as a driver of tourism competitiveness.

Digital Ethiopia emphasises delivering digital services using user-centred design and maximising the uptake and utilisation of digital public services.

4.6.2 Alignment with the ICT Sector Strategies

The Digital Government Strategy is also fully aligned with the Ethiopian government's sectoral strategies in key sectors like health, education, planning, finance (including Capital Markets), trade, agriculture, justice, and law and order. The Ministry of Health, for example, has been working on developing and cascading health information systems and digital health-related national documents based on national health strategy. These include the Information Revolution Roadmap II (2020- 2029), Information Revolution Strategic Plan (2018 -2025), Ethiopia eHealth Architecture (2019), and ICT Policy and Digital Health Strategy (2020-24).

4.6.3 Alignment with Sustainable Development Goals

The UN's Sustainable Development Goals (SDGs) guide the digital government strategy. Most strategic initiatives in the Digital Government Strategy are geared towards achieving SDGs, especially in reducing poverty, improving quality education and health, accelerating gender equality and promoting partnerships. Other SDGs addressed by this Strategy include SDG 9 (Industry, Innovations, and Infrastructure), SDG 10 (Reduced Inequalities), SDG 11 (Sustainable Cities and Communities), and SDG 16 (Peace, Justice and Strong Institutions).

The digital government strategy aims, among other things, to develop a digitally capable ecosystem. It also aims to improve the digital literacy of the workforce. Improvement in back-office systems such as Education Management Information Systems, eServices and digital skills can support quality education and increase the number of youth and adults with relevant skills, including technical and vocational skills, for employment, decent jobs

and entrepreneurship. The Strategy also emphasise equity and digital inclusion of women and people with disabilities, thus placing a strong emphasis on gender equity. User-centred digital government services will ensure that all men and women, particularly people experiencing poverty and the vulnerable, have equal rights to economic resources and access to basic services, ownership and control over land and other forms of property, natural resources and financial services.

4.6.4 Alignment with African Union Policies and Strategies

Regionally, the African Union Agenda 2063 guides the digital government strategy. The Strategy also considers the African Union Digital Transformation Strategy, the African Convention on Cyber Security and Personal Data Protection, the African Continental Free Trade Area and the African Data Policy Framework. It also takes the AU cybersecurity strategy and the draft Interoperability Framework for Digital ID, establishing the foundation for exchanging digital public services across borders. Special consideration is also made to the Continental AI strategy, Digital Education, Digital Agriculture, and Digital Health Strategies.

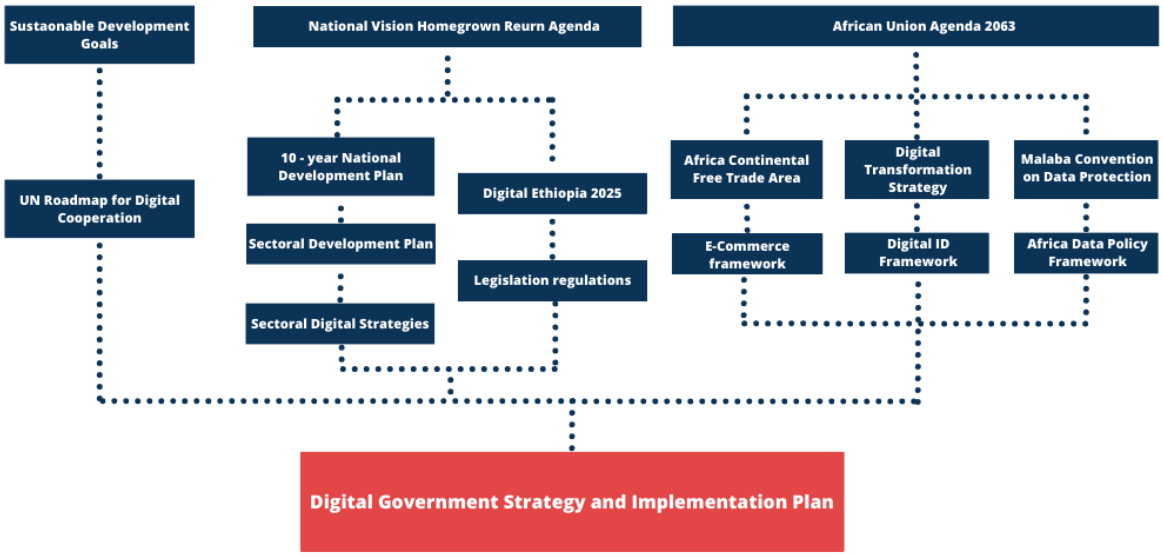

Figure 8: Digital Government Strategic Alignment

Part III: Pillars and Focus of Ethiopian Digital Government

5 The Architecture of the Digital Government Strategy

The Digital Government Strategy 2025-2030 will consist of:

- Digital Government Core – Application and Services including back-office automation, shared application, e-Services, access channels, registries and service catalogues
- Digital Government Foundations (enterprise architecture, emerging technologies integration, data, digital government infrastructure (cloud, GWAN, computing and software resources, digital ecosystem)
- Digital Government Enablers (change management, digital inclusion and eParticipation, legal frameworks, cybersecurity, coordination and governance)
- Digital Government Essentials (Financing and regional global dimensions).

The four strategic areas draw on eGovernment Strategies: the eGovernment Strategy (2010-2015), the eGovernment Master Plan (2016-2020), and international experience in digital government.

Digital Government applications and services are central to the government's work; therefore, these will be given priority in designing technology-enabled public services. The government will also ensure that the foundations of digital government and enablers are in place. Funding is a critical component of sustainable digital government; thus, innovative financing of digital government programmes will be identified through the engagement of citizens, development partners and the private sector.

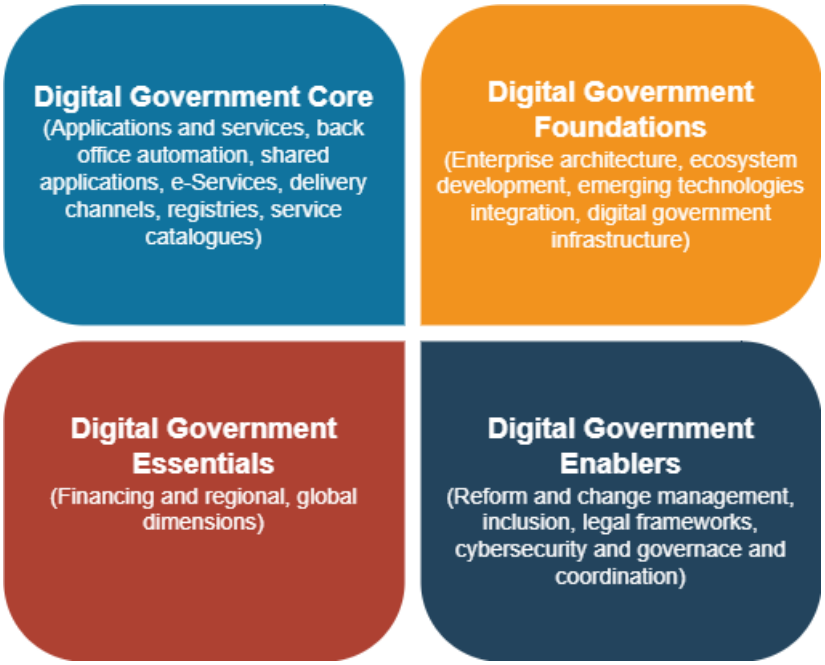

Figure 9: The Main Components of Digital Government

The detailed blueprint of the digital government strategy is shown in Figure 10. The blueprint makes users central to digital public administrations. It also emphasizes shared registries and components that draw on the digital public good and the Govstask approach.

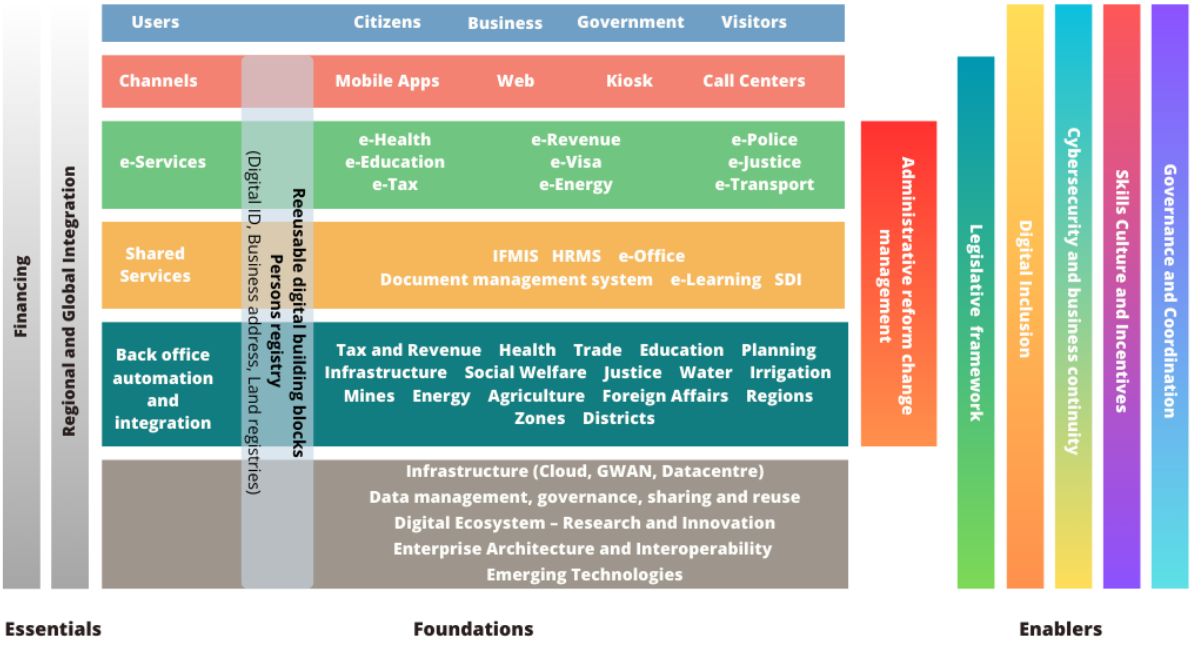

Figure 10: Digital Government Architecture

6 Digital Government Core - Promoting Digital Government Applications and Services

The digital transformation of government and public services starts with designing and improving back-office applications in ministries, departments, and agencies, as well as regional and local governments. All public institutions should adopt digital by default to ensure the availability of eServices to citizens and businesses through multiple channels. There is also a need for developing shared administrative management systems such as human resources management information systems, e-procurement systems, financial management information systems, and electronic office systems to increase the effectiveness and transparency of government administrative work, reduce costs, and eliminate duplicate re-creation of information systems with overlapping functions. Other critical applications and services include common applications such as web platforms, mobile platforms, contact centre platforms, and spatial data infrastructure (SDI) for collecting, storing, sharing, and managing geographic data to assist economic and social development.

The digital government application and services core will focus on enhancing service delivery through a whole-of-government approach, where data and resources are shared among government entities to provide end-to-end services. The focus will be on:

- Establishing a Centralized Digital Government Support Centre (DGSC) to manage the delivery of applications and services across the entire government,
- Ensuring all MDAs, regional governments, and local governments work closely to develop, implement and share their line of business back-office applications via Enterprise Service Bus,
- Ensuring all common and horizontal applications are developed and integrated with base registries and Enterprise Service Bus,
- Providing public-facing end-to-end online services to citizens, businesses, visitors and others by re-engineering government processes and applying user-centred designed principles,
- Delivering eServices using multiple channels, especially maximising the use of mobile technology to provide simple and easy access to online services.
- Incentivizing MDAs, regional and local governments in the delivery of eServices,
- Ensuring the foundations of digital government applications and services like Enterprise Service Bus, payment system, and core registries are in place and
- Driving users' adoption of eServices.

The government will invest strongly in the above areas, allowing for all the digital government principles in Table 5.

6.1 Establish a Centralized Digital Government Support Centre (DGSC) to Deliver Applications and Services

Experience of successful digital government indicates that the application of digital technology in the public sector is better coordinated when a dedicated centre is responsible for service design, standardisation, and technical support. The Ministry of Innovation and Technology will establish a Digital Government Service Centre (DGSC) responsible for delivering applications and services across the government. The DGSC, modelled around the experiences in Australia, Mauritius, New Zealand and the United Kingdom, will consolidate the current ad hoc digital government support provided by MInT, INSA and Artificial Institute to dynamic centralised capability. The DGSC will have highly skilled cohorts of versatile teams that support overall digital government transformation.

The Digital Government Service Centre, which will be an independent body reporting to MInT, should begin with a minimum of at least 120 strong experts covering all the technical domains of digital government like enterprise architecture (data, technology, application), networking, software development, mobile applications, data management and analytics, DevOps, API integration, end to end service design (User experience and User Interface design), user support and cybersecurity.

The Centre, among others, will:

- Support and maintain shared citizens and business portals,
- Support public institutions in their digitalisation effort through expertise (ad-hoc guidance, templates, documentation, etc.) and technical components (SaaS, PaaS, IaaS, etc.)
- Build and support common platforms, services, components, and tools based on the GovStack platform connected to the "EthioConnect" Enterprise Service Bus, discussed below.
- Support different entities in developing and executing an eServices implementation based on users and business journeys. The support will also cover how a particular MDA, regional or local government, applies an omnichannel method for service delivery.
- Devise and enforce minimum standards consistently across government digital services based on the Government Enterprise Architecture (GEA) and interoperability framework.
- Coordinate with the private sector by creating a GovTech lab platform that facilitates startups' active participation in the design and delivery of digital government solutions.

The DGSC's mode of operation will be established during the initial implementation phase of this Strategy. To ensure its sustainability, the government will recruit the best

talent, create rotating job roles, and introduce a progressive pay and talent retention strategy.

APS 1. Establish a Digital Government Support Centre

Actions:

- Develop a comprehensive plan and ToR for DGSC,
- Design incentive packages for staff,
- Establish a CIO position,
- Recruit, train and deploy experts in different digital governance applications and service areas, and
- Produce progress and annual reports on the operation of DGSC.

Outcomes:

- Sustainable and comprehensive support to digital government applications and services
- Improved user-centred services,
- Improved digital government innovation

6.2 Expand MDA' Line of Business Back-office Applications

MDA's back-office and management information systems are generally high-budget systems. Most MDAs have not implemented well-designed back-office systems to date; therefore, a backlog of MDA and regional government systems need to be developed and interconnected to a government Enterprise Service Bus. The existing back-office systems are not integrated into the workflow of the institutions and eServices. The current review indicates that:

- Most MDAs still use proprietary software systems, no rights to source code or system modifications,
- MDAs and regional governments are replicating expensive software systems and infrastructure already existing somewhere in government,
- Applications were not developed in conformance with Enterprise Architecture specifications,
- It was difficult to maintain quality standards on systems from a diversity of vendors, e.g., ERP solutions under development or trial by several MDAs and
- Some sectors or MDAs are better resourced than others in terms of computing resources,

Each Ministry, Department and Agency, regional and local government should develop a strategy for their overall informatisation that includes the development of the core line

of business back-office applications in conformance with the Government Enterprise Architecture and Interoperability Standards, GovStack specification and with connection to EthioConnect Enterprise Service Bus. Special attention will be given to shared applications and components and open standards to ensure data exchange between agencies.

Table 6: Typical Backoffice Systems with eService front ends

Ministry	Examples of Back-office Applications
Ministry of Foreign Affairs	• Immigration Information Management System • Visa Information Management System
Ministry of Peace	• Identity Management Information System • Disaster Management Information System • Early Warning System
Ministry of Finance	• Integrated Financial Management Information System • Aid Management Information System • Investment Tracking System • Asset Management System • Government Fleet Management System
Ministry of Justice	• Civil Status Information Management System • Judiciary Information System
Ministry of Trade and Regional Integration	• National Single Window • Business Licensing and Registration System • Import/Export Permit System
Ministry of Industry	• Licensing And Conformity System
Ministry of Innovation and Technology	• eProcurement System
Ministry of Urban and Infrastructure Development	• Construction Permits System • Real Estate Information Management System
Ministry of Water and Energy	• Digital Water System • Digital Energy System
Ministry of Tourism	• Integrated Tourism Information Management System
Ministry of Education	• Education Information Management System
Ministry of Health	• Integrated Health Information and Service Management System
Ministry of Women and Social Affairs	• Social Protection Information System

Ministry of Works and Skills	• Labour Market Information System
Ministry of Culture and Sport	• Cultural Information System
Ministry of Revenues	• Tax Management System • E-Customs System
Ministry of Transport and Logistics	• Vehicle Information System • Driver's License System • Logistics Information System
Ministry of Mines	• Mining Information System
Ministry of Agriculture	• Agricultural Information Management System
Ministry of Plan and Development	• Development Plan Monitoring System
Ministry of Irrigation and Lowlands	• Irrigation Management System

Regional and local government's back-office systems must be standardised and integrated with federal-level components based on GovStack specifications. The design and implementation of a back-office system must go through a careful requirement analysis, business process review, and data sharing and integration needs with other systems. Annex I presents a list of back-office systems that MDAs participating in the survey conducted during the preparation of this strategy have identified as important to their activities.

APS 2. Support the Development of Line of Business MDA Information Systems

Actions:

- Document the requirements, review business process, data access, sharing and integration requirements,
- Assess the adequacy and challenges with the current back-office system, if any
- Assess alternative open-source solutions,
- Ensure the applications conforms with GEA, Interoperability standards and GovStack specifications,
- Conduct, design, testing, users-acceptance and rollout of the new systems,
- Rollout and maintain the back-office systems taking data sharing, interconnection to Enterprise Service Bus into consideration,

Outcomes:

- Availability of open MDA information system that share data and reuse components,
- Improved delivery of eServices based on a well-designed back-office system
- Improved digital government services

6.3 Develop Shared and Common Platforms

The last decade has seen the rolling out of a series of common applications, including an Integrated Financial Management Information System and e-procurement system. However, these common applications remain standalone and not fully integrated. They do not share registries like a central digital ID. An effort has yet to be made to develop an e-office system comprising a series of efficient tools for managing document records and facilitating communication, promoting collaboration through centralised communications systems (email, chat, video conference). It is, therefore, essential to consolidate the current common application platforms, ensure that they align with the reference application architecture, and interconnect through an Enterprise Service Bus and GovStack building blocks. The GoE will also implement an e-office solution incorporating document management, knowledge management, records management, project management, messaging, and collaboration.

The eOffice solution will be critical to eliminating paper-based interactions within the government across different agencies. A document management system helps streamline internal processes to create a paperless office by migrating old documents from legacy systems to the archives. Dedicated email can be a very effective medium for inter-office and intra-office communication.

The government e-procurement solution[10] has already been used by many entities, with 228 participating in online procurement. The e-procurement app should be upgraded to facilitate vendor and procuring entities' management and support managing the bid process, contract management, and payments. A centralised Human Resources Management System will also be critical to managing public sector employees and improving efficiency and productivity. Efforts have been underway to develop a central human resources management. The GoE will:

- Upgrade and build Enterprise Resource Planning Systems like IFMIS, e-procurement, HRMS,
- Implement a comprehensive e-office system that comprises document management, knowledge management, records management, project management, messaging and collaboration,
- Build a Client Management System and
- Design, develop and upgrade other common platforms like ePayment, mobile platforms, and public online learning management systems.

This implies, on the one hand, there is a need to improve the current common applications by adopting open standards and solutions; on the other, there is a need to implement a comprehensive eOffice solution for the government to facilitate paperless delivery of services and foster collaboration. The following consideration can also be given to the design and deployment of common applications:

[10] https://egp.ppa.gov.et/egp/home

- Commonly requested systems will be best availed through a modern government cloud using a Software as a Service (SaaS) model.
- Common /popular applications can be developed with baseline functionality in microservices architecture and then customised and cloud-provisioned for line ministries, departments and agencies. Microservices enable scalable, modular and incremental development of the shared system functionality. Cloud provisioning of applications minimises ownership costs and improves online systems' performance, availability, reliability, scalability, and security.
- Office Business process and legal reviews and reengineering for improved efficiencies and workflow optimisation will be undertaken before the digitisation of each process or service. All work and business process flows and procedures must be documented.
- The EthioConnect Enterprise Service Bus can be modelled around the X-Road experience and can assist in orchestrating multi-step and multi-MDA eServices.

APS 3 Implement Cloud Based eOffice System that comprises document management, knowledge management, records management, project management, messaging and collaboration and event management

Actions

- Assess open standard solutions and make buy/build decisions,
- Development of ToR,
- International advertisement,
- Buy or build the e-Office to use EthioConnect ESB and comply with GEA and GovStack building blocks,
- Implement a comprehensive eOffice solution,
- Promote MDA and regional government adoption and training

Outcomes:

- Availability of comprehensive eOffice solution
- Progress towards a paperless government

APS 4. Develop and upgrade Major Enterprise Resource Planning (ERP) systems

Actions:

- Review of the current major ERP solutions such as IFMIS, E-Procurement, HRMS systems,
- Assess open standard solutions and make buy/build decisions,
- Develop TOR for core ERP improvement,
- Carryout international procurement ads
- Procure, build and upgrade core ERPs to use EthioConnect ESB and conform with reference application architecture and GovStack building blocks,
- Systematic implementation of GoE core ERPs (IFMIS, e-Procurement, HRMS) and
- MDA adoption, customization and training

Outcomes:

- Availability of cloud-based major government ERP solutions that conform to GEA and standards use GovStack building blocks (registry, identity, payment) and ESB,
- Improvement of sharing data across government to deliver better services.

APS 5 Develop a Government Client Management System

Actions:

- Develop Terms of reference for a modular Helpdesk, Customer Relationship, Service Feedback Management, and Complaints Handling System,
- Assess open standard solutions and make buy and build decision,
- International tender of the solution,
- Implement a government client management solution and
- Promote MDA and regional government adoption and training.

Outcomes:

- Availability of cloud-based government client management system provisioned as Software as a Service that conforms to GEA and standards, uses GovStack building blocks (registry, identity, payment) and ESB,
- Improved service delivery to citizens, businesses and visitors.

APS 6 Develop and Upgrade other shared platforms like Mobile, payment, SDI and eLearning

Actions:

- Analyse current shared platforms like mobile platforms, payment platforms, SDI platforms, and eLearning platforms for their adequacy for digital government services,
- Assess open standard solutions and make buy/build decisions for mobile platform, payment platform, SDI platform, eLearning platform,
- Upgrade mobile service delivery, ePayment, SDI, eLearning, and other application platforms.
- Procure or design and test the common platform - mobile service delivery, ePayment, SDI, eLearning, etc. based on users' needs and connection to EthioConnect ESB and in conformance with GEA and GovStack building blocks,
- Roll out and maintain common platforms - mobile service delivery, ePayment, SDI, eLearning, etc.

Outcomes:

- Availability of upgraded and shared platforms - mobile service delivery, ePayment, SDI, eLearning, etc.
- Improved government service delivery, and
- Increased adoption of the building block approach.

6.4 Develop and Deploy end-to-end eServices

The GoE plans to implement 2500 eServices by 2030. Rolling out these online services requires careful analysis of needs and prioritisation. The situation assessment indicates significant challenges with current eServices. Observations show that:

- The usage of current eServices is low. Currently, most eServices are intermittently available. MDAs use parallel or hybrid online and manual processes.
- Some eServices are not being used because of a lack of awareness and limited digital literacy.
- Almost all eServices do not incorporate customer feedback and complaint-handling processes.
- The design of eServices does not include business process transformation; thus, there is a tendency to digitise inefficient manual processes.

Therefore, building online services from a "whole-of-government" design perspective is essential. An eService rolling-out plan will be developed to ensure digital by default/digital-first principle. The services will be prioritised based on citizens' and business needs, language and localisation considerations, the volume of transactions of each service, potential utilisation rate and immediate benefits.

The government will roll out a service prioritisation plan that covers the following:

- Assessing the use of current eServices,
- Set targets for eServices delivery to ensure digital by default. The Strategy envisages that all Ministries, Departments and Agencies are required to plan and implement the changes needed to achieve targets of 80% of services online, of which at least 50% will be available as end-to-end services by 2030,
- Develop a comprehensive list of potential eServices to be rolled out by MDAs, regional and local governments,
- Rationalise the eServices via business process optimisation, eliminating obsolete services and unnecessary documents, consolidating related services and rolling them out based on businesses and users' journeys,
- Roll out eServices based on:
    - Identification of services to digitalise and institutions to be involved on an annual basis,
    - Localisation and language considerations,
    - Assessment of the institutions' readiness for service digitalisation and integration,
    - Analysis of citizens and business journeys, and
    - Service design, development, and integration. This includes designing and configuring e-service workflows, developing functionalities, ensuring integration of systems and databases, and incorporating eServices on the business and government portal,

- Develop a government-wide catalogue of eServices (e.g., including a brief description of each service, its fulfilment requirements, concerned government entities, and associated forms) to facilitate access.
- Ensure the proper running of the portal (infrastructure maintenance, incident management, etc.)
- Consider multi-channel delivery and
- Conduct training on the usage of the portal.

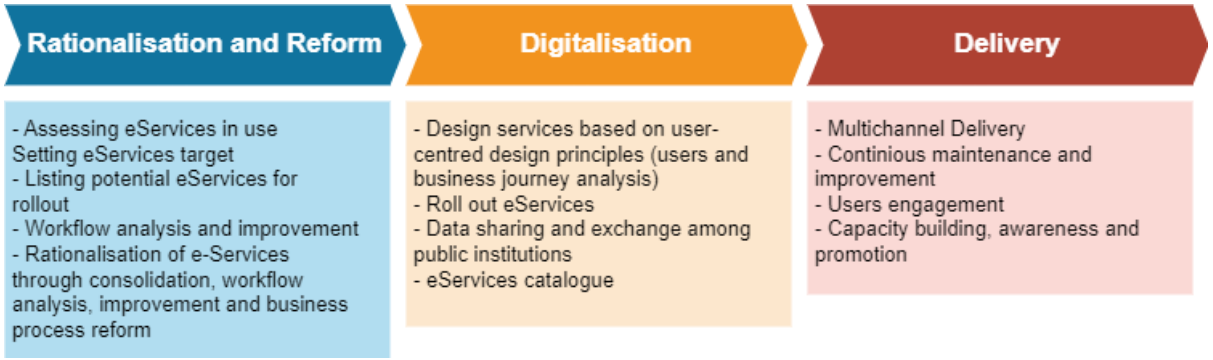

Figure 11: End-to-end Service Rationalization, Digitalization and Delivery Steps

The design and delivery of eServices will be based on user-centred design. The design process involves life event alignment, personalisation features, and user feedback accommodation. It consists of the following phases:

- Identifying with users.
- Identifying user needs and problems (through typical virtual personas, if necessary).
- Design innovative conceptual solutions based on user needs.
- Make prototypes - as the first phase in developing any service for citizens.
- Testing solutions with users.

A journey map is another key tool in user-centred design. It shows a user's journey through a service over time. It starts when a user's need for that service arises and ends when they stop using it. Services should also be organized around life moments concerning childbirth, schooling, employment, and old age care to proactively provide timely and correct information to people.

The user-centred design also means that all eServices take variations in location, connectivity, gender, skills, affordability and disabilities (or special needs), literacy, rural versus urban divide, age, and language into account. The GoE will also ensure that online end-to-end services comply with accessibility standards such as Web Accessibility Imitative (WAI) and Web Content Accessibility Guidelines (WCAG) standards and ensure eServices are mobile phone friendly.

APS 7- Develop and Deploy end-to-end eServices

Actions:

- Assess the use of current eServices,
- Set targets for eService delivery by all public institutions,
- Develop a comprehensive list of potential eServices to be rolled out by MDAs, regional and local governments,
- Rationalize the eServices via business process optimization, and ensuring conformance with a reference business architecture,
- DGSC, in coordination with MDAs and regional government, rolled out eServices based on user-centred design to reach targets set within the framework of digital-first principles, and
- Develop a government-wide catalogue of eServices.

Outcomes:

- Availability of user-centred eServices
- Availability of eServices catalogue
- Improved use of eServices

6.5 Transform eServices Access Channels

The provision of eServices should go hand in hand with increasing the channels through which these services are available to citizens and businesses. This implies increasing access channels for individuals and businesses, maximising the use of mobile applications and adopting the latest technologies to increase access and availability of services to different segments of society. Mobile phones play a critical part in citizens' daily lives. Developing mobile applications for selected eServices gives them a broader range of channels and greater convenience.

This strategy envisages that multiple technologies will access services, including websites accessible from computers and tablets, kiosks, mobile phone applications, and call and contact centres. Each government entity will conduct a detailed study to identify services that could take advantage of omnichannel delivery.

APS 8-eServices Access Channel Transformation and Omni Channel Service Delivery

Actions:

- Review of current services and users' channel use behaviour,
- Prioritize the development and implementation of mobile applications in conformance with the mobile-first principle, and
- Ensure that services are available through multiple channels.

Outcomes:

- Improved users' convenience, and
- Increased use of e-services.

6.6 Provide Incentive for Online Digital Government Service Delivery

The digital-by-default or digital-first principle requires that all government entities provide public-facing services via a government online portal. A legislative mandate requiring digitalisation over a specific period has been used to compel MDAs and other countries. Some other countries have used softer approaches, such as an "eGovernment Transformation Award" - a competition that awards excellence in end-to-end online service delivery.

The GoE will adopt the legislative and transformation award approach to incentivise end-to-end eService delivery. It will establish legislation that requires all public agencies to adopt digital by default within a specified period. It will also establish an eService transformation award that encourages online government service delivery and ensures cross-organizational knowledge sharing by showcasing success stories.

APS 9- Provide Incentive for Online Digital Government Service Delivery

Actions:

- Introduce guidelines and rules that require public agencies to provide services digitally by default within a specified period,
- Establish annual government award for successful digital government services,
- Publicize successful digital government services widely,

Outcomes:

- Increased availability of digital public service,
- Improved knowledge exchange and learning between MDAs, regional and local government on the delivery of excellent digital government services
- Recognition of good digital government service delivery that inspires the other agencies

6.7 Promoting the Foundations of Digital Government Applications and Services

Foundations like identity and payment systems and enterprise service buses constitute digital public goods and are the core components of the GovStack building blocks; thus, attention to these foundations will be critical to reducing the cost of digital public service and saving time and resources necessary to create digital services and applications. Building on the GovStack will help GoE to maintain consistency and quality of applications and allow agencies to speed up their delivery of cloud-based services by leveraging reusable common services, such as identity verification, payments, consent, digital registries, messaging, information mediation, scheduler and workflow. Participation in GovStack will also help the GoE learn from the experience of other countries in designing

and deploying digital government services. Through the GovStack community, the Government of Ethiopia could also leverage successful tools like Modular Open-Source Identity Platform (MOSIP) that is used for identity management, X-Road (for exchange of data), MojaLoop (for Payment), OpenCRVS (for Civil Registration) and OpenG2P (ID & Payment) and OpenSPP (Social Protection).

6.7.1 Establish Core Registries

The situation assessment indicates that data on citizen birth and ID, business, address, tax, vehicle, land, crime, licenses, and academic certificates are not readily available and are often duplicated. Users are required to submit data repeatedly on an ongoing basis, which has been one of the reasons for Ethiopia's lower EGDI score. It is therefore important to ensure all the key registers (digital ID, address register, land registers, vehicle and asset registers) are established, managed and organised using data and metadata standards. First, a data governance framework that outlines how to exchange, and who owns, manages and maintains specific data sets and registries needs to be established. Second, data should be shared between MDAs using the EthioConnect Enterprise Service Bus. Third, data must be exchanged between different entities for consistency and improved service delivery.

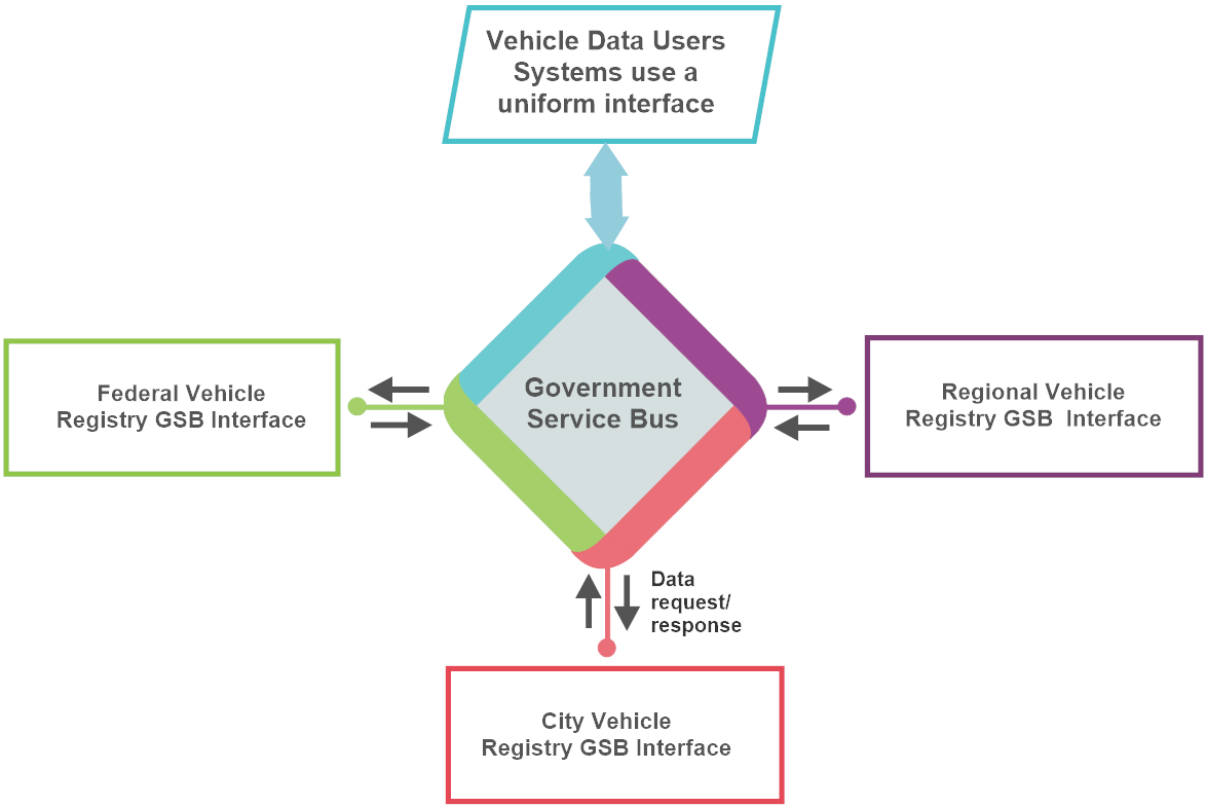

Figure 12: Example of Vehicle Data Exchange between federal, regional and city entities

APS 10- Establish and Expand Core Registries for Digital Government

Actions:

- Accelerate the adoption of Digital Identification as a basis for government service delivery,
- Establish data and metadata standards and identifiers that draw on international standards (for shared vocabulary, exchange, etc.) for all data and digital registries (digital ID, address register, land registers, vehicle and asset registers) to ensure sharing, interoperability and reuse,
- Establish governance framework for core registries data – designate who collects, maintains, keeps standards, shares including the MoU needed to share personal data between public sector entities,
- Use EthioConnect Enterprise Service Bus and Application Programming Interface for core data integration and exchange,
- Promote sharing and exchange of core registry data.

Outcomes:

- Increased use of digital identification for delivering public services,
- Availability of integrated and shared core registries,
- Adoption of standards for facilitating data exchange and sharing, and
- Increasing adoption of the EthioConnect ESB as a data integration and sharing platform.

6.7.2 Establish EthioConnect Data Exchange Platform

The situation analysis shows interest in interconnecting MDAs and regional and local governments' isolated applications and systems. Interoperability between government systems is typically ensured through an Enterprise Service Bus that connects applications services and base registries, facilitating the exchange and sharing of data.

The Enterprise Service Bus is a system integration and interoperability software platform that removes the need for direct connections between two interacting systems. Connections and service requests are sent to the ESB rather than directly to the MDA system that implements the service. This provides location independence to all services. There are commercial and open-source versions of Enterprise Service Bus platforms. Still, governments are increasingly adopting open-source ones like the X-road, which is now available in over 20 countries. The Zambia Government, for example, has adopted an Enterprise Service Bus known as ZamConnect, based on an open-source X-Road platform launched in June 2020, and more than 40 services have been integrated into it so far.

The Ethiopian government will follow suit with the experience of these countries and establish the EthioConnect Enterprise Service Bus to allow the exchange of data between information systems of all MDAs and regional and local governments and connect with information systems of the private sector. The basic motivation of an ESB system is not just to provide the institutions with a standards-based data exchange eServices delivery platform but also to provide a structured and managed system-to-system communication for the exchange of data and, through it, a single market for all Government data and eServices. ESB enables aggregations of services and the

elimination of effort duplications and inefficiencies in ways that are impossible in point-to-point integrations. For example, an Ethiopia Investment Promotion Authority system can have simultaneous access to the company registry, ID registry, revenue authority system, ePayment switch and the construction and business permit registries. The figure below illustrates how Ethiopia MDA's digital systems could collaborate via an ESB.

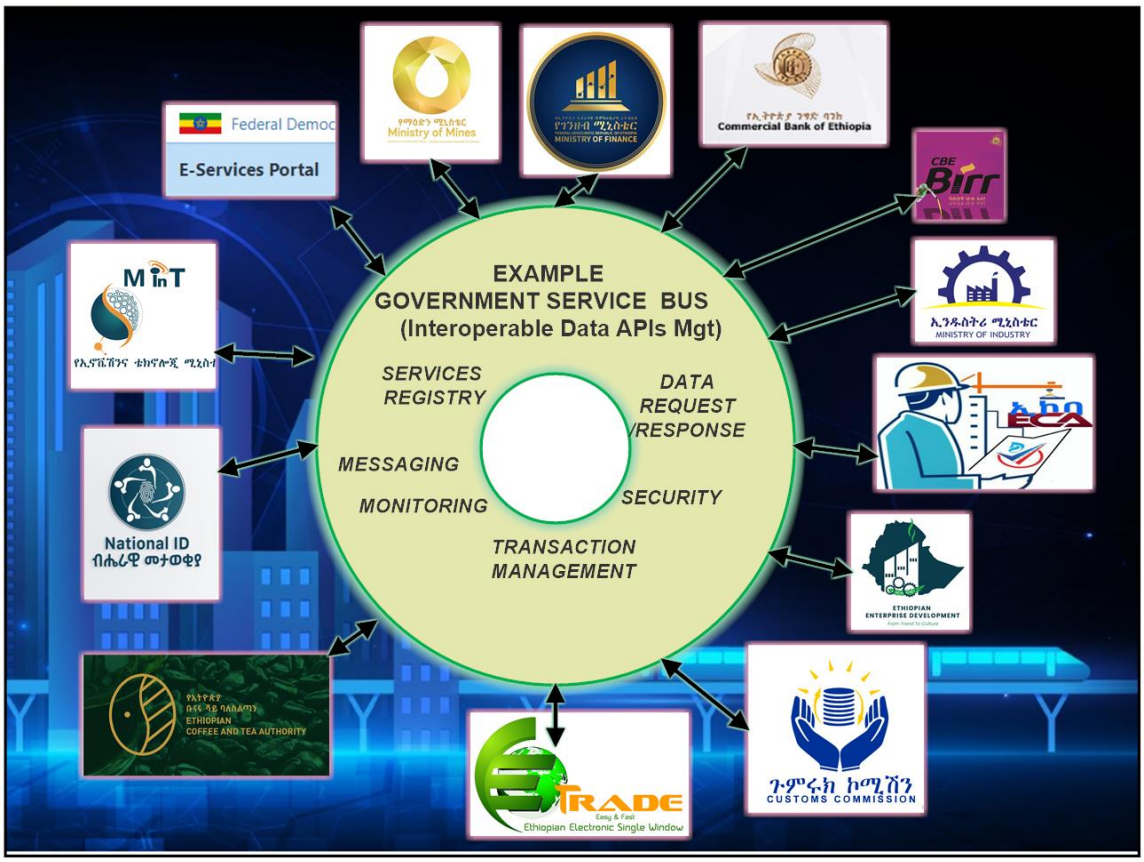

Figure 13: Example of Service Integration Via Enterprise Service Bus

APS 11- Establish EthioConnect Enterprise Service Bus

Actions:

- Develop the Terms of Reference for the EthioConnect Enterprise Service Bus,
- Explore open source and commercial solutions,
- Adopt and implement the EthioConnect ESB and publicize it as a brand,
- Integrate Pilot MDA, regional and local government service providers to EthioConnect ESB taking Reference Integration Architecture into consideration,
- Build the capacity of DGSC to integrate services via the ESB.

Outcomes:

- Availability of EthioConnect ESB,
- Integration of core registries and selected MDA services into the ESB and

- Accelerated digital public service through shared data.

6.7.3 Diversify and Accelerate Digital Payment System for eServices

The situation analysis shows significant progress in financial inclusion by introducing mobile payment services (Telebirr and MPesa) in recent years. However, more must be done to improve digital payment integration in government service delivery. Integrating online payment to eServices will facilitate payments to the government, reduce waste of time and improve convenience. It will also promote government to citizens' payment, improving financial inclusion and economic empowerment. Integrating the mobile payment system is specifically useful because it will promote end-to-end service, reduce direct costs to the government, reduce fraud and corruption, increase convenience for recipients, and create pathways to financial inclusion.

Thus, all eServices must incorporate digital payment, especially mobile payment systems. This implies building and improving the digital payment system infrastructure for public services through the connection and use of the national payment gateway and ensuring the effectiveness, security, convenience and confidence in the payment methods for eServices. Each eService should assess better payment channels, mobile, e-banking and credit/debit cards to foster inclusive and efficient online payment that considers beneficiary choice and convenience.

APS 12- Diversify and Accelerate Digital Payment System for eServices

Actions:

- Assess the use of existing payment systems for digital public service, including convenience and users' challenges,
- Improve the payment infrastructure – national payment gateway and ensure security and effectiveness, diversify digital payment models (mobile, e-banking, debit/credit card, etc.)
- Encourage MDA's regional and local governments to switch to digital payment for all services.

Outcomes:

- Availability of diverse digital payment systems that increase convenience and quality of government services,
- Improved revenue collection, and
- Improved financial inclusion and empowerment.

6.8 Consolidate eService Delivery Portals

Progress in the centralised portal <eservices.gov.et> has been steady, with over 350 services currently available for businesses, citizens and visitors. However, the user base is small, and the number of eServices with end-to-end transactions is limited. Besides,

multiple portals for transactional services run in parallel, providing fragmented services, most of which are used by multiple government entities and institutions (e.g., e-Trade). Thus, it is important to consolidate all the available portals from MDAs and regional governments into a few core portals providing seamless government services, e.g., central government portal, business and trade portal, investment portal and open data portal. Portals should also be organised based on users' end-to-end journeys.

Creating a Digital Government Support Centre is expected to alleviate the challenges of limited capacity at MInT, limited user-centred design, and inadequate tracking of the performance of eService portals. Through the Digital Government Support Centre, the GoE will consolidate national portals to provide end-to-end services for citizens, businesses, visitors, investors and other entities. The number of portals will be kept to a minimum to facilitate resource sharing and provide a one-stop-shop for users.

APS 13- Consolidate eServices Delivery Portals

Actions:

- Assess the use of existing portals that are available from MDAs, regional and local governments,
- Assess whether the portals conform to national standards, GEA, design best practices and accessibility standards,
- Develop a plan for consolidation and harmonization of government portals with end-to-end services into the account,
- Consolidate all portals into central government portal, business and trade portal, investment portal and open data portal, leveraging Reference Integration Architecture and ESB and
- Organize eService portal based on end-to-end business, citizens, visitors, investors journeys.

Outcomes:

- Availability of central government portals that provide stop-end service,
- Improved user convenience,
- Optimal use of technical and human resources, and
- Enhanced delivery of government services.

6.9 Drive Users' Adoption of eServices

The situation assessment shows the usage of eServices is very low compared to the number of services available on the national portal. Experience in other countries has shown that encouraging users to 'have a go' is the best way to drive adoption. Promoting online channels that are convenient to users, such as mobile apps, can also increase adoption. Incentives like making transactions involving online transactions cheaper than offline or providing quicker turnaround for online transactions can also drive adoption. Ensuring that users are fully aware of the benefits of online services (for example, easier

tracking of the status of applications, auditability, and possible time saved) can also drive usage.

It is also important to establish trust in electronic services. Users want to know that their transactions can be completed securely online. This means their data is handled per defined privacy and security principles and can only be accessed by authorised agents. The GoE will conduct an ongoing audit of service usage and devise strategies for increasing users' adoption of online services.

APS 14- Accelerate Users' adoption of eServices

Actions:

- Assess the use of existing eServices and identify users' adoption challenges,
- Accelerate users' awareness of available eServices through publication and wider dissemination of eServices catalogue,
- Introduce incentives like making it cheaper and faster to get services online and
- Improve trust in end-to-end eService, including security and data protection.

Outcomes:

- Improved use of eServices,
- Increased convivence and access, and
- Improved government services, revenue and empowerment of citizens.

Digital government concerns mainly the delivery of application and services, thus prioritising the activities outlined above is crucial for the implementation of the Strategy. Prioritisation is generally difficult because, the expansion of MDA applications should go along with availing eServicices, which in turn depends on consolidating portals and promoting users' adoption. However, it is important to sequence these actions in order to allow stakeholders to focus on short-, medium- and long-term goals. Figure 14 presents a prioritisation of these actions in a time horizon between 2025 and 2029.

Figure 14. Prioritisation of Application and Services

Application and Service Actions[11]	2025	2026	2027	2028	2029
Establish a Centralized Digital Government Support Centre (DGSC) to Deliver Applications and Services					

[11] Key – Red Priority, Green – priority and requires ongoing activity, Yellow- work is already underway

Expand MDA' Line of Business Back-office Applications					
Implement Cloud Based eOffice System that comprises document management, knowledge management, records management, project management, messaging and collaboration and event management					
Develop and upgrade Major Enterprise Resource Planning (ERP) systems					
Develop a Government Client Management System					
Develop and Upgrade other shared platforms like Mobile, payment, SDI and eLearning					
Establish Core Registries					
Establish EthioConnect Enterprise Service Bus Based on X-Road Experience					
Diversify and Accelerate Digital Payment System for eServices					
Develop and Deploy end-to-end eServices					
Consolidate eService Delivery Portals					
Transform eServices Access Channels					
Provide Incentive for Online Digital Government Service Delivery					
Drive Users' Adoption of eServices					

Part IV: Digital Government Foundations

7 Foundations of Digital Government

Digital Government cannot function without a reliable digital infrastructure. Other foundations, such as a robust data ecosystem, the ICT enterprise, research and innovation environment, and enterprise architecture and standards, are essential for the success of digital public services. Data is increasingly becoming a foundation for digital government; therefore, its governance, management and use are important for effective public service delivery.

Governments are also adopting emerging technologies to support digital public services. Emerging technology generally refers to a new or continuing development of existing technology that is expected to be available within the next ten years and create significant social or economic benefits. Such technologies that significantly affect digital government include Artificial Intelligence (AI), additive manufacturing (3D printing), augmented reality, autonomous vehicle systems, blockchain, cloud computing, data science, robotics, and the Internet of Things. Artificial Intelligence, blockchain, and IoT have now become general-purpose technologies with far-reaching impacts on the functioning of governments.

8 Modernisation of Digital Government Infrastructure

National digital infrastructure is a foundation of public sector transformation. In this Strategy, digital infrastructure activities involve:

- Modernisation data storage and hosting infrastructure- data centres,
- Cloud enablement,
- Modernisation and upgrade of Government-Wide Network,
- Modernisation of institution-level Networks, and
- Accelerating broadband connectivity for all.

An analysis of the state of digital government infrastructure indicates the need to upgrade a national data centre and implement a comprehensive business continuity and disaster recovery plan, transition to a cloud environment, upgrade the WoredaNet to IP-based Government Wide Area Network and increase access to affordable broadband connectivity across the country. In addition, there is a need to improve MDA and regional governments' Local Area Networks and enhance public procurement of hardware and software to ensure the latest, reliable and energy-star devices are available to public institutions.

8.1 Rationalise, Upgrade and Consolidate Government Data Centres

The GoE offers shared technology infrastructure for its core operations through a national data centre (NDC) operated by MInT, Ethiotelecom, AI & INSA. However, not all MDAs and regional governments are connected to the NDC; some ministries invest in their infrastructure, and others plan to build new data centres. Lack of data centre rationalisation and consolidation has created a fragmented environment that already led to inefficient storage and hosting capacity in government and wastage of resources across the public sector. Moreover, the NDC was not upgraded using industry standards and was inefficient in its service delivery. Current demand from a few MDA exceeds the NDC's capacity to deliver.

Moreover, the MInT does not have a disaster recovery site or a business continuity plan. There is no data backup retention policy and no dedicated backup server. This has created a significant challenge for government business continuity. Thus, it is important to upgrade the Government Data Centre and establish a disaster recovery centre to increase the effectiveness and productivity of the government, reduce costs and maintain data security. A data centre rationalisation strategy is required to interconnect or retire all existing data centres at the MDAs and regional government to ensure better and more responsible maintenance, protection, and data sharing.

The main activities will then include:

- Upgrade of the current national data centre that meets the Uptime Institute Tier III standard,[12] with ample storage and state-of-the-art functionality. This may entail construction of an all new data centre.
- Establish a disaster recovery facility to facilitate business continuity,
- Develop an MDA data centre consolidation plan to create a shared services environment.

The GoE has already launched a national data centre upgrade plan through the World Bank's Digital Foundation Project.[13] The bid is expected to result in a full upgrade of the NDC and the construction of a disaster recovery site; therefore, this activity is not considered in this digital government strategy. However, upgrading the data centre and establishing the disaster recovery site should be accompanied by analysing the consolidation and interconnection of existing MDAs and regional government data centres.

DGF 1 – Rationalise and Consolidate Government Data Centres

Actions:

- Review the status of data centres at MDAs and regional and local governments,
- Assess technical, connectivity and usage issues that affect existing data centres in the government,
- Assess the applications running on these data centres and the potential for upgrade to the cloud or migration to the national data centre or other optimised public and private data centres,
- Develop a data centre consolidation plan based on Reference Technology Architecture and metrics such as cost saving, energy saving, etc.
- Implement a data centre consolidation and rationalisation plan.
- Develop disaster-resilient infrastructure strategies, particularly for the National Data Centre and Wide Area Networks (WANs).
- Assess feasibility of a new modern National Data Centre.
- Integrate renewable energy sources to power IT systems, aligning with the principle of environmental responsibility.

Outcomes:

- Government cost saving,
- Interconnection, collocation and resource sharing,
- Improved energy savings, and
- Acceleration of a whole of government approach.

[12] https://uptimeinstitute.com/tiers

[13] https://projects.worldbank.org/en/projects-operations/procurement-detail/OP00230655

8.2 Accelerate Cloud Transition

The Government of Ethiopia realises the importance of cloud computing in delivering effective digital government services. Cloud technology will improve public sector resilience and business continuity during crisis and recovery capabilities and enable the GoE to keep up with technological development. Building public sector solutions with the latest cloud computing resources and tools ensures that governments keep up with the private sector.

While developing a national data centre is essential, cloud transition will be important, especially when digital services reach a reasonable maturity level. A hybrid model combining an independent on-premise data centre with cloud services will be considered initially. This will allow data classification to ensure hosted services on the internal government network and other data via the cloud. By adopting a hybrid approach, the government will be able to cut down on administrative overhead, streamline IT workflows and deploy new software features faster.

The many benefits of cloud have prompted many governments to move to cloud computing and introduce cloud-first policies. Cloud-first policies mandate that government agencies and departments prioritise using and procuring cloud systems by default where a secure, reliable, and cost-effective cloud computing option exists. MDAs and regional governments that opt for the cloud must conduct a risk assessment and data classification to allow different types of data to be managed on-premises and via the cloud and build their internal capacity.

Cloud enablement demands that the GoE improves its current procurement policies to allow for utility-based variable cost items, decide on data localisation issues, adopt a cloud computing strategy and build its internal capacity in this area. The Government will develop a cloud enablement strategy and ensure in-house cloud capacity is built within the Digital Government Support Centre. The DGSC cloud computing team will establish a government cloud platform, share knowledge, resources (e.g., common code and services) and best practices (e.g., in procurement and migration), and support MDAs' regional and local government's gradual migration to the cloud.

DGF 2- Accelerate Cloud Transition

Actions:

- Develop a cloud computing strategy that addresses security, business, technology, skills and cultural considerations and requirements with a clear implementation plan,
- Review current policies and legal frameworks to ensure policies and legislations support cloud enablement,
- Build in-house capacity within the Digital Government Support Centre,
- Encourage data classification, risk assessment and gradual cloud migration, and

- Promote ongoing cloud transition.

Outcomes:

- Improved public sector resilience, business continuity,
- Improved capability to keep up with technological development, and
- improved cost saving.

8.3 Modernise Government Wide Area Network

The GoE has operated a backbone Network (WoredaNet) for the last 16 years. WoredaNet is a terrestrial and satellite-based communications network that provides Internet connectivity and other services such as video conferencing and messaging to federal, regional, and woreda-level government entities. While WoredaNet originally served as a Government-Wide Area Network, its functionality as GWAN was degraded due to low-capacity equipment and bandwidth. Connectivity between the MDAs and regional government is offered through the Ethio Telecom network,. Further, it was difficult to monitor security risks associated with connectivity. The GoE has already initiated a programme to modernise the WoredaNet network. Therefore, this activity is expected to be undertaken by the World Bank's Digital Foundation Programme.[14]

i. First, there is a need for a comprehensive redesign of the WoredaNet into a full-fledged government Wide Area Network that ensures high speed and reliable connectivity to public institutions at federal, regional, zonal, district and lower levels. A two-stage design process is proposed, starting with Software-Defined Wide Area Networks (SD-WAN) - a transitional arrangement for digital services to government bodies. This approach will reduce the overhead costs and increase network performance, improve application performance and increase agility whilst a government IP Core network is being built. Next, the GoE must build an IP core network that will serve as an underlying network for government interconnectivity. A GWAN that is built on an IP core network will reduce transmission costs, improve the quality of services and reliability and provide secure delivery of Government-to-Government (G2G), Government-to-Business (G2B) and Government-to-Citizen (G2C) services.

ii. Second, there is a need to enhance the network's bandwidth to support digital government solutions and interaction, including video conferencing. Typical government networks run between 5Gbps and 100s of Gbps. Thus, setting a minimum bandwidth that will be required at Kebele, district, zone, region, and MDA levels is important. Benchmarks like the number of users can be used to estimate bandwidth requirements at different levels. Global benchmarks in the education sector indicate tha a minimum of 1 Mbps per user bandwidth is typically

[14] https://projects.worldbank.org/en/projects-operations/procurement-detail/OP00238717

recommended; thus, a Woreda with over 100 staff should at least have a 100 Mbps connection. The government must continuously improve connectivity to ensure the bandwidth meets the growing demand of civil servants, businesses, and citizens who use the network.

iii. Third, the network needs to be built to be resilient, able to adapt to failures and resume normal operations when the failure has been resolved. It should conform to the GEA's Reference Technology Architecture and Reference Resilience Architecture. This implies that the network design should include redundant components and links. Different technologies, including wireless networks, point-to-point microwaves, TV white space, fibre, and satellite-based broadband networks, should be incorporated into the design to facilitate the network's resilience.

iv. Fourth, the network's security should be considered since the GWAN is a national critical infrastructure.

DGF 3 – Modernise WoredaNet to Establish IP Core Government Network

Actions:

- Redesign WoredaNet and establish a secure and resilient IP Core Government Network based on a Reference Technology Architecture,
- Improve bandwidth of all government institutions, and
- Designate the Government Wide Area Network as critical infrastructure and enhance its security.

Outcomes:

- Improved access to secured and high bandwidth government services,
- Improved capability to keep up with technological development,
- improved cost saving, and
- Enhanced government services.

8.4 Modernise Institutional Local Area Networks

Local Area Networks (LANs) at MDAs, regional governments and local government levels will be considered because these often pose a significant challenge in delivering user services. Due to their poor design and operations, these networks are often the main bottleneck in the connectivity chain. Most government offices have Local Area Networks with varying quality and reliability issues, making accessing back-office applications, printers and the Internet difficult. These networks are crucial because public sector staff devices must connect through a local wireless or wired network to access the Internet, back-office systems, printers and other essential resources for the day-to-day delivery of services for businesses, citizens and visitors.

Public sector Local Area Networks must be designed to meet the security, connectivity, and performance challenges while enabling access to applications and services. They must conform to the Reference Technology Architecture and the Reference Resilience Architecture of the Government Enterprise Architecture. They must scale as needed and offer operational simplicity and flexibility to accommodate new computing trends.

It is important to train technical experts at MDAs' regional and local governments to ensure smooth network operations. Organisation-specific specialised boot camps and design workshops will be useful to ensure that these networks are designed and implemented to meet the growing demand for efficient public services. Workshops and boot camps can also be platforms for sharing experience on network design, cabling, security, network operation and monitoring issues.

DGF 4 – Modernise Institutional Local Area Networks

Actions:

- Establish a standardised framework for institutional local area networks design and implementation based on a Reference Technology Architecture,
- Develop network design capabilities of the IT team at MDA and regional government,
- Invest in standardised tools for network monitoring and management, and
- Ensure MDAs, regional and local governments develop and enforce Acceptable Network Use Policies.

Outcomes:

- Improved access to secured and high bandwidth government services,
- Improved capability to keep up with technological development,
- improved cost saving,
- Enhanced government services.

8.5 Accelerate Broadband Connectivity in Rural and Underserved Areas

Low-level broadband penetration and intermittent and slow Internet are some of major factors contributing to the low usage of digital public services by citizens. Internet penetration in Ethiopia is low at 39.2 %, with a 34.8% 4G/5G coverage a concentrated in major cities and towns. As the government aims to ramp up the digitisation of services, universal high-speed and quality broadband and affordable devices across the country remains vital.

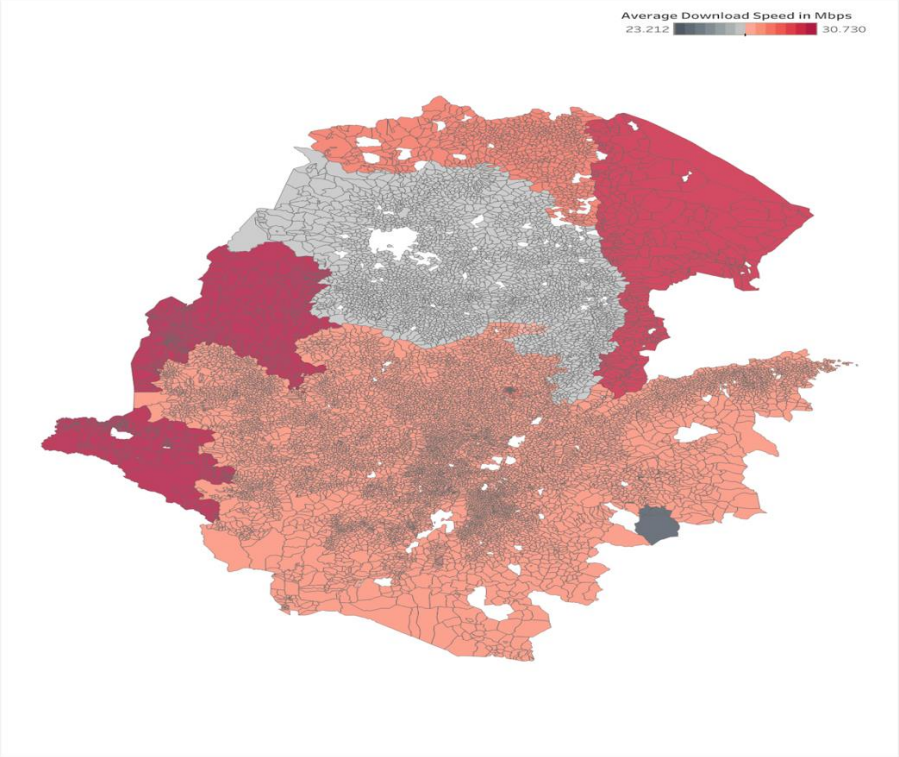

Figure 15: Variation of Download Speed Across Different Parts of Ethiopia

Accelerating broadband connectivity to all corners of Ethiopia is needed to provide equitable digital government services. This demands that Ethio Telecom, Safaricom, and the Ethiopian Telecommunications Authority (ETA) collaborate to expand broadband in underserved areas by developing and implementing a broadband strategy. It also implies that expanding links to fibre optics networks to ensure half of the population access to it within 25 Km radius and accelerating access to broadband wireless services, including rising from 4G from 34.6% to universal coverage and 5G from under 1% to 10% by 2029.

Ethiopia should seriously look into the immediate deployment of satellite broadband internet technology, with control and licensing regimes suitable for Ethiopia. It is noteworthy that satellite broadband internet connectivity in some of Ethiopia's African peers has connected the remotest villages and schools to fast internet overnight.

DGF 5 – Accelerate Universal Access to Broadband Connectivity

Actions:

- For immediate 100% broadband coverage, explore immediate deployment of satellite broadband internet technology, with control and licensing regimes suitable for Ethiopia.
- Encourage operators to extend network coverage in commercially viable areas,
- Update broadband strategy to accelerate satellite, fibre and broadband wireless (4G and 5G) access to citizens,
- Promote the connection of digital infrastructure at local levels, such as to kebele offices, schools, health centres, and towns, to support digital public services, and

- Use the Universal Service Fund to subsidise broadband connectivity to areas that are not commercially viable, particularly underserved and unserved locations in rural areas.

Outcomes:

- Increased access to reliable and secure government services,
- Digital inclusion and empowerment of all citizens, and
- Improved delivery of digital government services.

9 Adopt Enterprise Architecture and Interoperability for Connected Government

Enterprise Architecture (EA) provides a holistic infrastructure, data integration, and application blueprint for government; therefore, it is considered one of the foundations. EA defines, organises, and standardises business processes, data, applications and technology. Interoperability enables connections between MDAs, sectors, and countries through data, information systems, legal agreements, organisational processes, and shared values.

The Government of Ethiopia developed a National Enterprise Architecture Framework (NEAF) in 2011. The NEAF (GEA 1.0) defines government service, application, data and technologies architectures, the governance and legal and regulatory framework and the application, technology, data and security standards and specifications.

The Government was not able to implement GEA 1.0 due to the absence of a proposed governance framework that facilitates interaction between MInT (led by lead architects) and IT directors and application development team leaders at MDAs, lack of skills in enterprise architecture and interoperability across Ministries, Departments and Agencies. In 2019, the School of Information Science at Addis Ababa University (AAU) reviewed the GEA 1.0. It emphasised the need to establish a governance structure and define and adopt architectural principles and technical standards. Meanwhile, there has been a significant shift in the EA approach from "building" to "enabling", from “system” to “ecosystem”, and from a standard framework for designing enterprise architecture that typically takes months and years to agile enterprise architecture that delivers in weeks.

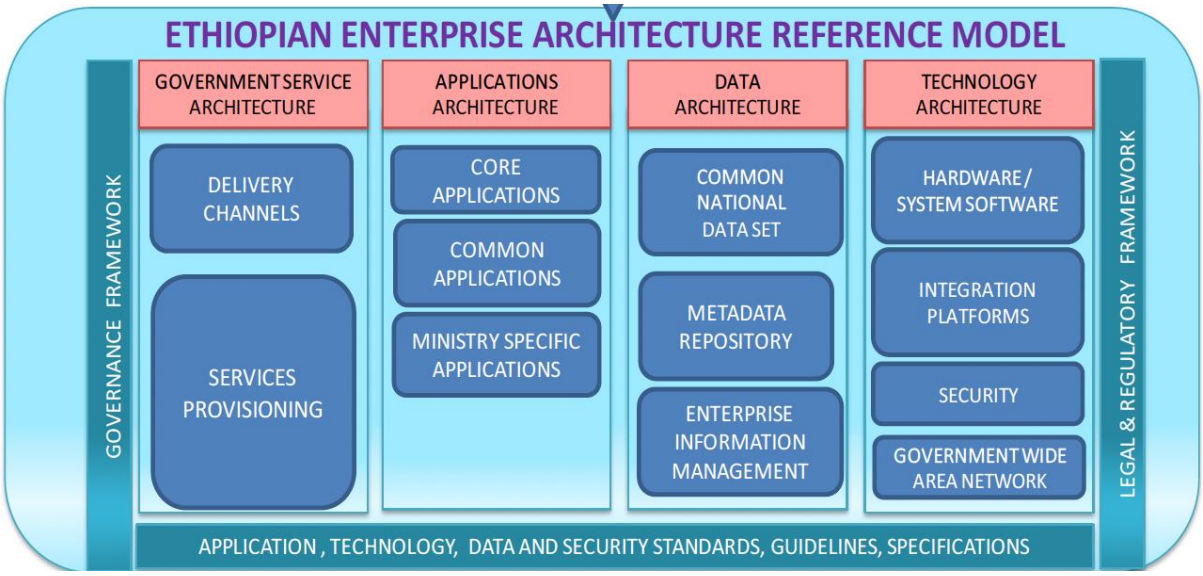

Figure 16: The National Enterprise Architecture Framework (GEA 1.0) Reference Model

GEA 2.0, which accompanies this Digital Government Strategy, builds on the Ethiopian Enterprise Architecture Framework and eGovernment Interoperability Framework GEA 1.0 and TOGAF components but provides modifications and enhancements to the application, technology, security, data, governance and integration reference architectures with a focus on the building block and ecosystem approach to facilitate cross-organisational reuse of applications, services and implementation. GEA 2.0 adopts the GovStack building blocks – like registries, identity and payment that interact with other building blocks through well-defined and stable APIs.

GEA 2.0 emphasises federated architecture, openness, cloud-first, mobile-first, privacy-by-design and security-by-design principles. It outlines federated architecture with national, whole-of-government and sectoral (MDA) tiers to suit the needs of different administrative structures and simultaneously build a connected government.[15]

[15] Government of India, IndEA 2.0, https://www.meity.gov.in/writereaddata/files/InDEA%202_0%20Report%20Draft%20V6%2024%20Jan%2022_Rev.pdf

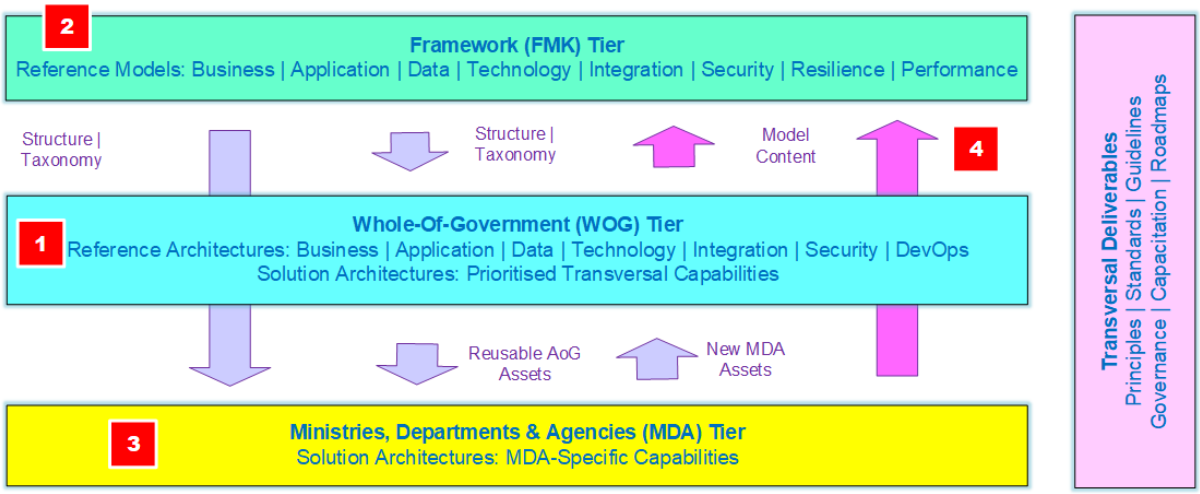

Figure 17: GEA 2.0 Framework

GEA 2.0 implementation will be ensured when MDAs and regional and local governments achieve meaningful interoperability. Achieving truly interoperable government requires overcoming change management issues and adhering to a mix of technical, semantic, legal, organisational, and cultural norms. Non-digital interoperability aspects like governance, legal frameworks, institutional and individual incentives and skills are critical. Technical aspects like data readiness, data architecture, increased use of Application Programming Interfaces (APIs), presence of Enterprise Service Buses (ESB) and open standards and open source are also essential.

The implementation of GEA requires establishing a governance framework that aligns with the overall digital government coordination framework outlined in the Strategy's Governance section. This includes establishing a Digital Government Support Centre that will host enterprise architects (business, data, application and technology architects) and pursue the implementation of the GEA 2.0 roadmap. Adopting cloud computing, cyber security and business continuity strategies will also be crucial for implementing GEA 2.0.

Developing interoperability and enterprise architecture competency is another crucial aspect of successfully implementing GEA 2.0. Efforts will be made to build capacity and develop the competencies of government staff and IT professionals at MDAs and regional governments to perform and execute user-centred digital public service.

GEA 2.0 recommends that government staff should receive training in various topics such as data policies, governance and protection, federated architecture, building blocks, service design, business analysis, internetworking issues, and the role of emerging technologies. Professionals should also receive in-depth training on concepts of digital governance, federated architecture, data design, management, analytics, governance and protection, building blocks, system integration standards, service design, business analysis, internetworking, security and privacy, emerging technology integration and programme management. Given the speciality of this subject domain, experts should deliver GEA 2.0 capacity. The GoE will use multiple delivery channels, including face-to-

face in-person training, online learning, peer-to-peer learning, boot camps and workshops, and a certification programme to upgrade enterprise architecture skills.

DGF 6 – Implement Enterprise Architecture and Interoperability Framework for Connected Government

Actions:

- Adopt the GEA 2.0 and implement its Roadmap,
- Adopt federated architecture and begin with the Whole-of-Government Tier, and establish MDA and other minimal architectures based on requirements,
- Adopt technical interoperability standards,
- Accelerate interoperability by ensuring non-digital and digital interoperability aspects,
- Establish GEA 2.0 governance as part of digital government governance and coordination framework,
- Build the competencies of government staff and professionals.

Outcomes:

- Improved interoperability of government,
- Accelerated whole-of-government approach and
- Improved delivery of digital government services.

10 Accelerate Data Management and Sharing

Data is an important part of everyday life and essential to providing citizens and businesses with the necessary services and information. Using data helps improve healthcare and scientific research, creates new opportunities for the education sector, enhances production workflows, promotes innovative government action, and makes everyday life easier. Good data is essential for the government to produce stronger and better-informed policies and improved delivery of effective, equitable and inclusive services. The COVID-19 pandemic highlighted the importance of making high-quality data accessible to the population.

The government of Ethiopia collects a wide range of data, either in paper form or in a digital format. A vast amount of data is currently being generated through transactions between citizens and the government. However, this data is not organised and accessible; thus, it is not used fully. Data are often dispersed across fragmented registers (datasets used by government entities for a specific purpose), which are often managed in organisational silos. The situation assessment of government data handling shows that data are routinely stored in diverse (magnetic, paper) formats that are hard to process. Many institutions lack the skills to process data. Data also contain sensitive personal information or business secrets; therefore, part of such data must be protected. The absence of data protection law also implies that citizens have little transparency on what data the government stores about them or how it is used.

Making data more accessible to people, businesses, academia and policymakers and optimising its use through integration enables everyone to do their work more efficiently. People can make decisions to improve their quality of life if they have greater access to the right data and tools to extract insights. Effective use of data supports better government services and drives competition and economic growth, especially in creating jobs within the private sector. There is a growing use of data by security forces such as police from various new sources to protect infrastructure, citizens and businesses. But this should be done by respecting fundamental and property rights.

There are various steps to increase data use in the government. First, the data needs to be identified and categorised. There are numerous ways that data can be categorised. A primary distinction is between personal data and non-personal data. Registries, for example, are data sets that are important for the functioning of government, but they often have personally identifiable data elements. Digital IDs, business registries, land registries, and address registries are important basic sets of data that should be collected, organised and shared across government. Non-personal data are generated from disaggregated statistics, satellites, and Internet of Things (IoT) devices. Data from operators such as Internet Protocol Detail Record (IPDR), Data Detail Record (DDR), and

Call Detailed Record (CDR) are also increasingly becoming an important tool for decision-making.

The GoE realises that effective governance, policies, regulations, and legislation should protect data. Attention will also be paid to accessing quality, interoperable, and reliable data – primarily from the government in open data format but also from the private and other sectors. The capacity to analyse, visualise and use data is also critical.

There are a wide range of data and data sources:

- The government is the main data generator but also plays different roles in the data cycle (generate, collect, store, analyse, use, share and preserve data). Government data centres focus on storing and preserving it.
- Universities and research institutions focus on generating, collecting or analysing data; researchers produce some data but typically take data from the public and private sectors and add value through integration, aggregation and analysis to provide societal benefits.
- The private sector also collects customer data for planning and operational purposes. For example, the communication sector generates anonymous data such as Internet Protocol Detail Record or Data Detail Record and Call Detailed Record that are critical for understanding tourism development, population mobility, and pandemics. Mobile call Detailed records or Data Detailed Records have already shown that they can play a critical role in managing pandemics and serve as early warning tools during natural disasters.
- Data can also be generated from IoT sensors, such as machines that can be added to traffic poles, temperature gauges that can be installed on boilers, etc., and satellite systems. Machine-based data is increasingly important for economic growth, environmental protection, safety, and disaster response.
- Location data is another important element in facilitating different commercial and public services. Accurate location data is key for intelligent transportation, electronic commerce, and emergency response. Businesses and citizens need timely access to trusted and accessible location data for investment to protect assets and make decisions for their communities. Governments need authoritative and timely location data to target community investment best and deliver various public services.

An inventory of data sets will be carried out, and a governance framework will be established to collect, process, store and disseminate data. This will create transparency on the existing data assets and enable the government to establish a data pool that supports decision-making. The government will also remove barriers to managing, sharing, and reusing data and apply data to transform public policies and services' design, delivery, and monitoring. Open data principles will ensure that citizens and businesses make the best of non-sensitive data sets. Implementing the Personal Data Protection Law (Proclamation No. 1321/2024) will also be critical to protect citizens and make them aware

of their data rights regarding security and transparency of use. The following actions will be used to increase the value of data:

10.1 Conduct Inventory of National Data Sets

A national data sets assessment was carried out in 2015 that identified 188 of the most common datasets that meet the established criteria of commonality and more than 500 potential common datasets for inclusion from ministries, departments, and agencies. The list is now out of date, and the proposed data sets may have already been available or discontinued; therefore, it is important to launch a programme that assesses what the government has and the gaps in terms of conversion and standardisation and making them available for public, private and government use. Mapping will allow the GoE to "know what it knows" and what data is available and where. It will also enable the government to assess where critical data is lacking and where data is stored in multiple registers. The data sets assessment will enable the government to develop a data atlas that enables easy finding of government data and facilitates more collection, conversion, sharing and reuse of data, including making open data available for citizens, the private sector and research. Establishing national data sets will enable the government to make data accessible at a higher quality level, which will benefit industry, academia, civil society as well as the public sector itself, unleashing the creative potential to tackle development challenges.

DGF 7 – Conduct Inventory of National Datasets

Actions:

- Conduct a comprehensive assessment of national datasets based on the 2015 survey and Reference Data Architecture,
- Establish a national data atlas and data pool,
- Develop strategies for the digitalisation of non-digital data, and
- Define a plan for data standardisation, provision, storage, integration, analytics and use.

Outcomes:

- Increased availability of data, including core registries,
- Increased use of data for decision-making, research and advocacy, and
- Increase innovation and use of open data for economic development.

10.2 Establish a Data Governance Framework

A data governance framework is essential to designate who collects, manages, maintains and shares data. Governance provides mechanisms for data flows between government, non-government organisations, and businesses. It will ensure data quality, integrity, security, availability, harmonisation, legal and regulatory frameworks, and overall data

management. The government will implement strong governance mechanisms to coordinate cross-agency and regional, zonal and district government data efforts by establishing inter-jurisdictional forums.

The GoE will also ensure accurate and timely data on persons, businesses, assets, land and vehicles are gathered and shared across government entities. It will also enhance the management and sharing of national spatial data. Other sectoral sub-registries will also be established based on the core registers to facilitate data reuse. In addition, mechanisms for creating data identifiers (for instance, individuals, companies, or buildings) are needed to facilitate the unambiguous and efficient connection of data stored in different sources.

Data standardisation covers aspects such as processing (raw data, processed data, curated data), the completeness of data (i.e., missing values) and the granularity of the data (level of detail and frequency of availability) and open specifications and standards for different sectors including education, transport, statistics, environment, agriculture and food, meteorology, and geodata. The GoE will facilitate the development and adoption of data and metadata standards and common data structures in these core sectors to facilitate data sharing and exchange.

DGF 8 - Establish a Data Governance and Sharing Framework

Actions:

- Establish a governance framework for data that outlines who collects, manages, maintains and shares government data and includes standards for data quality, interoperability, and security.
- Establish and implement a data quality framework through a data governance framework,
- Create data identifiers and standards in core sectors, and
- Promote data sharing and exchange.

Outcomes:

- Formal framework for collection, management and sharing in place,
- Enhanced data quality and sharing,
- Increase in evidence-based policymaking, and
- Increase innovation and use of open data for economic development.

10.3 Promote the Availability of Open Data

The government holds a significant amount of data, most of which would benefit citizens and businesses if released. Studies show that investment in open data, including publicly funded research, generates a return on investment of 1.5 times. The GoE has been participating in global open data partnerships. Some institutions have started initiatives

to open data, but there is a lack of coordination at the central level. The GoE will take steps to prudently publish open data that is in demand in a usable format to increase transparency in public services, facilitate research and analysis and generate economic value.

DGF 9 – Promote the Availability of Open Data,

Actions:

- Assess current online open data available from MDA,
- Classify data available from national data sets study into open and non-open data, and
- Ensure all open data is published through the open data platform.

Outcomes:

- Increased availability of open data,
- Increased use of data for decision making, research and advocacy, and
- Increase innovation and use of open data for economic development.

10.4 Increase Data Analytics and Use

Data will only have value with use; thus, promoting analytics and use is essential to transforming data for digital government. The growing availability of data presents intense demand for skilled workers, including data engineers, data scientists, data analysts, and those who can bring a data-driven perspective to government. Citizens also need data literacy to judge and use data competently and innovatively by themselves. Data literacy is the ability to identify data sources, collect and organise data, and understand, analyse, interpret and present data. It also covers a basic understanding of the right to informational and applicable data protection rules.

The government will promote data analytics and use it by investing in data infrastructure, skills, and capabilities. It will launch programs for data analytics and use at all levels, especially in key sectors like education, health, justice, law, and order. It will boost data science capabilities and harness analytical tools and techniques (including machine learning and Artificial intelligence) to predict service needs, gain efficiencies in agency operations, support evidence-based decisions and improve user experience.

DGF 10 – Increase Data Analytics and Use

Actions:

- Assess current data use by citizens and businesses,
- Devise and implement programs for data literacy, data analytics and use in government, especially in key sectors like education, health, justice, law and order, and
- Support data science programmes in higher education.

Outcomes:

- Enhanced data analytics and use,
- Increase in evidence-based policymaking, and
- Increase innovation and use of open data for economic development.

11 Accelerate the Use of Emerging Technologies for Delivery of Public Services

Emerging technologies, including Artificial Intelligence, big data analytics, blockchain, cloud computing, and the Internet of Things, have reshaped government digitalisation in recent years.

- Artificial Intelligence refers to the development of computer systems that can perform tasks that typically require human Intelligence, such as learning, problem-solving, and decision-making.
- Blockchain is a decentralised digital ledger that securely stores transactions and data across a network of computers, ensuring transparency and immutability. With its secure and transparent nature, blockchain can enhance data management, automate processes through smart contracts, and facilitate cross-agency collaboration.
- Big data analytics involves uncovering trends, patterns, and correlations in large amounts of raw data to help make data-informed decisions. It uses familiar statistical analysis techniques—like clustering and regression—and applies them to more extensive datasets with the help of newer tools.
- Cloud computing is an on-demand delivery of IT resources (servers, storage and applications) with pay-as-you-go pricing. Instead of owning or buying servers, storage or applications or maintaining physical data centres, government agencies can access technology services such as computing power, storage, applications and databases from cloud providers. The Cloud Computing model comprises five essential characteristics (viz. on-demand self-service, ubiquitous network access, metered use, elasticity and resource pooling), three service models (infrastructure as a service, platform as a service and software as a service), and four deployment models (public cloud, private cloud, community cloud and hybrid cloud).
- Internet of Things refers to devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.

In recent years, governments worldwide have started to recognise the potential of these emerging technologies for enhancing public service delivery and fostering citizen engagement. Adopting these technologies in digital public service helps streamline processes, increase efficiency, and improve the overall quality of public services. Thus, it is important to integrate these technologies gradually into government services.

Table 7: Example of Emerging Technology Use in Government

Emerging	Potential Application in Government Services

Technology	
Artificial Intelligence	• AI-powered Optical Character Recognition (OCR) systems can automatically process and verify documents, saving time and reducing manual errors. • AI improve the delivery of public services by automating routine tasks, reducing wait times, and personalizing services for citizens. • AI can enhance the government's data-driven approach by enabling more effective data analysis and decision-making. • AI-driven chatbots and virtual assistants can provide 24/7 support for citizens and businesses, answering frequently asked questions, guiding users through processes, and assisting with form submissions. • AI can help reduce time-consuming, labour-intensive, repetitive administration tasks like managing transport flows, • AI plays a great role in language translation and the correct way of writing documents. • AI as a tool to enhance cybersecurity measures, which aligns with the objective of creating a secure government. • AI facial recognition tools can be used for the identification of criminals, • AI can analyse large datasets to identify patterns, trends, and correlations, providing valuable insights to inform policymaking. For example, AI algorithms can analyse transactions and behaviour patterns to detect and prevent fraudulent activities in various government sectors, such as welfare programs, taxation, and procurement.
Blockchain	• Blockchain can securely store and verify digital identities, reducing fraud and theft. For example, blockchain-based land registries can help multiple parties securely hold copies of the registry. Securely, his model could help quickly resolve property disputes or prevent corruption. • Blockchain-based identity management can be used to certify e-voting and online tax returns, • Customs and border protection widely use blockchain because it provides quicker, more reliable attribution about the origins and legitimacy of shipments and goods, • Blockchain-based smart contracts can automate and streamline procurement processes, reducing corruption and bureaucracy. • Blockchain is widely used in personal records like certificate authentication with multi-layer security and real-time detection of potential breaches, • Blockchain can eliminate intermediaries and reduce bureaucracy, leading to more efficient government processes.
Big data Analytics	• Government data from tickets, videos, tweets, etc., can be subjected to big data analysis to predict population movements, user preferences, transportation details, and more as a basis for decisions.

	• Big data analytics can be used to examine financial data for detection of fraud and tax evasion, • Big data analytics can use data from unusual conversations, texts, interactions, contacts, purchases, or movements in potentially dangerous locations to identify criminals. • Data from hospitals, accident reports, disease centre reports, social services case files, and geo statistics can help determine where there might be a greater need for medical or social services • Data collected from transport routes can be used to oversee transportation to ensure better roads, safer roadways, better routes and new routes.
Cloud Computing	• Cloud computing transforms how IT is consumed and managed, resulting in improved cost efficiencies, accelerated innovation, and the ability to scale applications on demand. • Cloud-based services can help protect sensitive information, simplifying projects and collaborations and ensuring business continuity in the event of a disaster
Internet of Things	• IoT can be used for law enforcement since law enforcement personnel can't simultaneously be present at all high-risk locations. IoT-enabled surveillance systems can provide continuous, real-time intelligence. • The government can use IoTs to manage a full range of infrastructure, including building roads and bridges, power grids, water supply lines, gas supply, rail lines, airports, etc. • IoT plays a key role in disaster management - IoT sensors can be set up in forests to detect fires in their early stages to curb their spreading and the consequent devastating effects. IoT can also help in areas prone to flooding by monitoring the water bodies to alert authorities when the water levels rise at alarming rates. • IoT can be crucial in transport and traffic management and planning. • Using magic bands, people can have all their identity information and important information updated and secured

Adopting these and other emerging technologies in the public sector requires that the GoE prepare strategies to accelerate their use and ensure that the necessary platforms are created for experimentation. The GoE will also need to invest in people (digital skills), secure and affordable infrastructure, and establish an enabling environment for investment and local ICT sector's innovation in this disruptive area. There is also a need to invest in advanced digital infrastructure, including 5G networks, government cloud, data centres, and other Internet resources. The accelerated use of emerging technologies requires the following:

11.1 Develop National Strategies for Emerging Technologies

The GoE has not yet developed strategic guidelines for artificial Intelligence, cloud computing, blockchain and data analytics. It is, therefore, important to initiate processes to develop either a combined strategy for these emerging technologies or individual strategies for Blochian, Artificial Intelligence, and IoTs. The Government will review global practices in developing strategies for core emerging technologies and develop and implement appropriate strategies through public consultation.

DGF 11 - Develop National Strategies for Emerging Technologies

Actions:

- Develop national strategies for emerging technologies - AI, blockchain, IoT, big data analytics and Cloud Computing,
- Conduct public consultation on emerging technology strategies, and
- Adopt and implement emerging technology strategies for AI, blockchain, IoT, big data analytics and Cloud Computing.

Outcomes:

- The availability of well-developed strategies that guide emerging technology use in the economy in general, in the public sector, and
- Full integration of emerging technologies in the economy and public service delivery.

11.2 Create Platforms for Engagement on Emerging Technologies

The GoE realises that applying emerging technology in the public sector requires a critical mass of innovators who interact regularly to exchange knowledge and issues around the solutions they are working on. Thus, platforms that bring innovators are critical to nurture innovation in this growing field. Forums such as blockchain, AI, and IoT working groups that meet regularly and discuss innovation and opportunities will be established to ensure those interested in these subjects work together.

DGF 12 – Create Platforms for Engagement on Emerging Technologies

Actions:

- Create platforms for engagement on emerging technologies, and
- Encourage virtual and face-to-face meetings on different topics of emerging technologies to pitch solutions and exchange knowledge.

Outcomes:

- Availability of forums for emerging technology innovators,
- Acceleration of innovation in core emerging technologies, and
- Improved availability of emerging technology products and services.

11.3 Develop Emerging Technology Skills and Research

Investment in advanced AI, blockchain, big data analytics, IoT and cloud computing skills is critical for competitiveness and accelerating their application in government. This can be achieved by:

- Upgrading the secondary education curriculum focusing on science, technology, engineering and mathematics (STEM) education will ensure that young people graduate high school with an introduction to these technologies.
- Integrating emerging technology courses in computing and engineering curriculum to train a critical mass of youth in blockchain, 3D printing, Artificial Intelligence, augmented reality/virtual reality, robotics process automation, biotechnology, big data analytics, Internet of Things and automated and connected vehicles.
- Developing and delivering fast-track emerging technology short courses to upskill the current youth with core digital skills in web design and networking. This can be achieved by organising regular hackathon events to explore the application of new technologies, including Big Data, Blockchain, Open Data, Artificial Intelligence, and other topics in government.
- Launching research and development on emerging technologies- There is a need to launch research in all essential emerging technologies to promote cooperation among research and technology centres and generate synergies and collaborations among national, regional, and global researchers.

DGF 13 – Develop Emerging Technology Skills and Research

Actions:

- Upgrade the curriculum in secondary education to introduce concepts of emerging technologies,
- Integrate emerging technology courses in computing and engineering curriculum,
- Develop and deliver fast-track emerging technology short courses for government IT staff,
- Launch research and development on emerging technologies.

Outcomes:

- Increase awareness of emerging technologies,

- Availability of critical mass of experts in emerging technology,
- Improved research and development and innovation in emerging technologies

11.4 Promote Regulatory Sandboxes and Financial Incentives for Innovative Emerging Technologies Solutions

ICT Regulatory Sandbox is a pre-emptive framework that creates an agile regulatory environment to launch innovative ICT services and solutions. The government will create regulatory sandboxes to ensure the applications of emerging technologies are treated before being rolled out for use in the public sector.

The GoE will also provide fiscal incentives for emerging technology enterprises and researchers, including initial risk funding from the universal access fund or research and development fund for emerging technologies startups and entrepreneurs to enable them to develop innovative applications and solutions. The government will also support the commercialisation of products and services through grants, scholarships, venture capital, etc.

DGF 14 – Promote Regulatory Sandboxes and Financial Incentives for Innovative Emerging Technologies Solutions

Actions:

- Promote regulatory sandboxes for testing emerging technologies, and
- Provide financial incentives for emerging technology innovators and startups.

Outcomes:

- Availability of regulatory sandboxes that encourage innovation,
- Availability of financial incentives for emerging technology startups and innovators,
- Increase in critical mass of emerging technology experts and innovators, and
- Availability of innovative digital government solutions that leverage emerging technologies.

12 Development of Digital Government Ecosystem

The ecosystem around digital government includes the ICT private sector, academia, and civil society, which are engaged in advancing public services. The private sector and academia play significant roles in advancing digital public services. Other stakeholders, including digital innovation hubs, entrepreneurship centres, and civil society, are also important in digitalisation.

The Government realises the limited civil society organisations that advocate for improved digital public services and an innovation hub environment. Cultivating the innovation hubs, entrepreneurship centres, and forums is critical for competitiveness and improved digital government solutions that meet local challenges. Open participation and discussion among government, the private sector, civil society, and academia is essential to boost innovation, education, and entrepreneurship.

12.1 Advance the Private Sector and Startup Ecosystem

The private sector will have a critical role in digital government in developing innovative technology solutions and supplying tools, platforms and services. It possesses the technical expertise and experience to implement complex digital systems and often moves faster in deploying products and services, thus contributing to the transformation of digital government.

While the local private sector has grown in recent years, it still needs to improve in delivering advanced government services. The startup ecosystem is at its early stages, with a few companies able to move from the inventing of products and services to commercialisation and profitability. Efforts to support local startups are underway, but often, there is no match between digital government challenges and startup solutions. The GoE also realises private sector startup efforts are only sometimes geared towards solving public sector solutions. Thus, it is important to undertake initiatives that target and strengthen the local private sector and improve startup's ability to create innovative solutions that meet national challenges. The financial sector could also play a key role in providing capital for innovation (loan and credit facilities, venture capital and supporting public and private partnerships. The Government will take the following actions to foster the capabilities of the local private sector:

- **Promotion of collaboration between the public and private sector through GovTech Labs –** the government will create regular forums to align public sector problems with innovators' products and services and promote the participation of the private sector in the design and implementation of digital public service solutions. It will explore public-private partnerships on digital innovations and

solutions in hardware, software, content and emerging technologies like AI, blockchain, big data analytics, IoT and robotics for public administration.

- **Revision of procurement rules** to provide incentives for local private sectors' participation in the delivery of innovative government solutions,
- **Fostering the startup ecosystem** by strengthening support services like innovation hubs and accelerators and providing technical and financial incentives like training, protecting intellectual property, and establishing connections to investor networks. This also includes expanding opportunities for startups through sandboxes and increasing their participation in public procurement.

DGF 15 – Advance the Private Sector and Startup Ecosystem

Actions:

- Promote public and private partnerships on digital innovations,
- Revise public procurement rules to create incentives for local private sector participation and
- Create a conducive environment for startups.

Outcomes:

- Increased private sector participation in the delivery of advanced digital government solutions and
- Improvement in the startup ecosystem and gradual graduation of innovators to enterprises.

12.2 Promote Academic and Research Sector for Digital Government

Ethiopia has several public and private universities with academic programmes in digital technologies. Still, the quality of the institutions varies based on the level of knowledge and concepts imparted in the classroom, programming skills developed while in college and the extent to which concepts and coding skills are used for problem-solving. Universities largely focus on concepts, with light attention to coding and limited or no focus on problem-solving. Besides, colleges and universities do not provide high-level skills, especially in emerging technologies topics (e.g., blockchain, cloud, IoT, AI, data analytics).

Digital research and innovation are key strategies for increasing the capacity, effectiveness, and efficiency of digital transformation in government. Therefore, improving the academic and research environment for digital government is essential.

- Develop a digital government research plan and designate universities that serve centres of excellence in core digital government areas (e.g., GovStack building

blocks, cybersecurity, legislations, emerging technologies integration, process reform, etc.),

- Accelerate entrepreneurship and commercialisation of research solutions by supporting the evolution of universities as digital solutions incubation and acceleration hubs,
- Reform curriculum and integrate problem-solving as a core competency and advanced ICT industry skills (e.g., blockchain, cloud, IoT, AI, data analytics) relevant to public sector digital innovation.

DGF 16 – Promote Academic and Research Sector for Digital Government

Actions:

- Develop a digital government research plan and designate universities that serve centres of excellence in core digital government areas,
- Accelerate entrepreneurship and commercialisation of research solutions in universities and
- Reform curriculum and integrate problem-solving as a core competency and advanced ICT industry skills.

Outcomes:

- Improved innovation, research and digital products and services that are incubated in universities and
- Increase in critical mass of digital solutions and emerging technology experts and innovators.

Part V: Digital Government Enablers

13 Enablers of Digital Government

To succeed, the digital government needs enablers like coordination and change management, digital skills and culture, cybersecurity and business continuity, inclusion and effective regulatory framework.

- Coordination and governance are key because the lack of effective strategy ownership leadership across government ministries and agencies can undermine digital government implementation.
- Digital skills and a civil service culture in a digitalised environment are essential prerequisites for modern online public service.
- Regulatory frameworks provide the basis for protecting the rights of citizens' businesses and improving trust in digital public service; thus, they are enablers for accelerating the use of eServices.
- Transforming public administration processes is important to leverage digital technology to deliver effective and efficient services.
- Cybersecurity and business continuity enable the sustainable functioning of online government.

14 Whole-Of-Government Governance/ Policy Support/ Coordination Framework

Digital government is a national challenge that requires a high level of coordination. Government plays a key role in setting strategic objectives, facilitating the enabling environment, providing resources and incentives, setting standards, and monitoring and evaluating digital government progress. The assessment of the current governance environment shows that coordination is a main issue in the implementation of digital government in Ethiopia due to diverse actors implementing different programmes, priorities, strategies, goals, and plans in silos. The eGovernment Strategy 2011 and the eGovernment Master Plan of 2016 propose the following coordination framework:

- The Council of Ministers headed by Prime Minister to be the Program sponsor,
- A High Committee under the Minister of Innovation and Technology is to be established for the effective implementation of eGovernment,
- Technical committees to be established to discuss and deliver various aspects of digital government and
- A Digital Government Project Management Office is to be established within the Ministry of Innovation and Technology.

These governance mechanisms are not fully in place except for the central sponsorship of digital government by the Prime Minister's and Deputy Prime Minister's Office. International experience shows that digital government is better implemented when a central entity, typically a ministry, provides strategic guidance, coordination and execution and when an institution that designs services maintains standards and norms exists. The Ministry of Innovation and Technology plays a strategic role, but the GoE lacks an institution that provides overall technical and operational guidance and support for digital government. The Digital Government Support Centre, recommended (APS 1) above, will be a key to building and supporting common platforms, services, components, and tools and provide digital expertise support for all government entities.

Experience of successful countries indicates that a lean and collaborative governance model is desired. Thus, it is important to reduce the number of entities involved in digital government implementation to a minimum. At the same time, a whole of-government approach ensures maximum participation and widened ownership from government entities and stakeholders. The Digital Government Strategy proposes a governance structure shown graphically below that comprises:

- Central sponsorship and leadership by the Council of Ministers and Prime Minister,
- A Digital Transformation Council,

- Six Thematic (Sectoral) Technical Committees on Digital Government,
- Ministry of Innovation and Technology and Digital Government Support CentrePlatform for coordination of Digital Government Initiatives across MDAs, Regional Government and Local Governments,
- Project Technical Working Groups,
- Coordination platforms with the private sector and academia

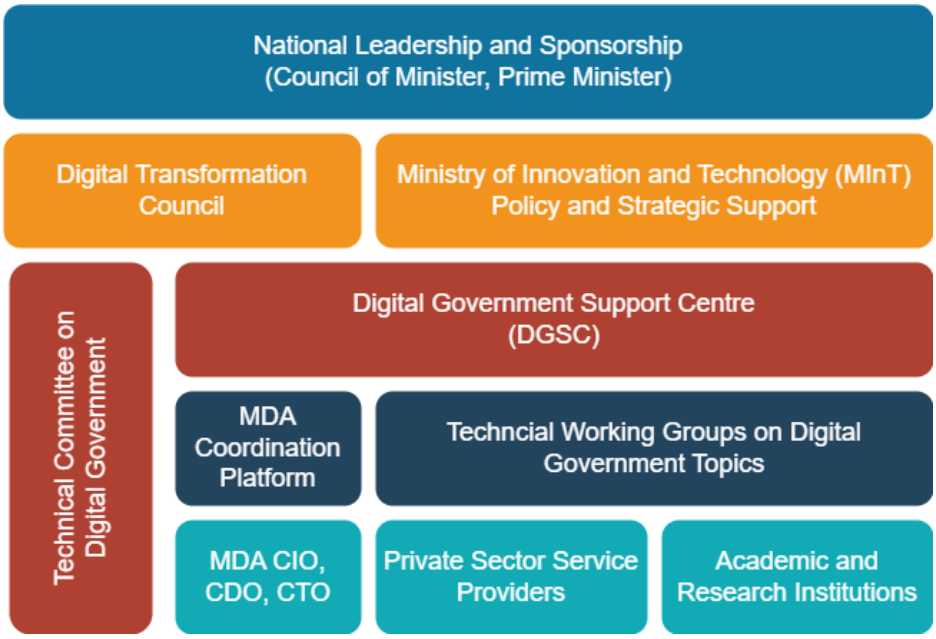

Figure 18: Proposed Governance Framework

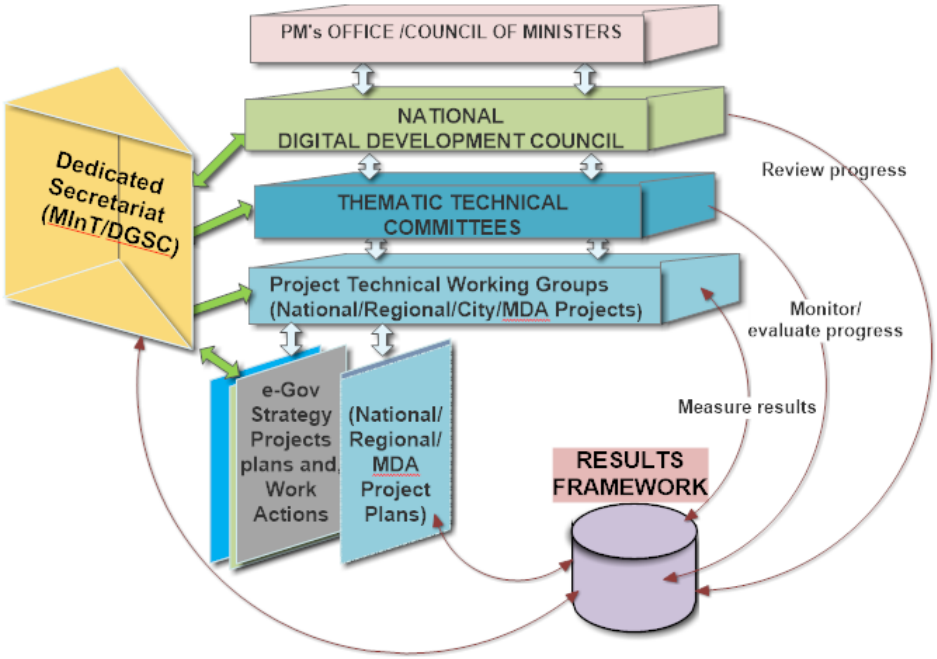

Figure 19: Proposed Governance Framework Hierarchy

This governance framework will be implemented to integrate digital strategies with national economic policies, particularly HGER 2.0 and the Ten-Year Development Plan.

14.1 Promote National Leadership and Sponsorship

A high-level sponsorship of digital government is critical because sponsorship is at the highest level behind every successful digital government programme. Strong collaborative leadership from the top creates the foundational conditions for effective digital government. The digital government programme requires ongoing support from the Prime Minister, the Council of Ministers and the leadership of Ministries, Departments, Agencies, and regional and local governments. Decision-makers need to push for change, make resources available, publicly take "ownership" of the digitalization of services and commit their time on a sustained basis. It should also be noted that leadership waits for results, so efforts should be made to deliver user-centred, data-driven and whole-of-government services. There is a need for ongoing awareness-raising workshops for leaders on digital public service data, technology, usage and security topics tailored to their settings.

DGEN 1 – Promote High-level Leadership and Sponsorship of Digital Government

Actions:

- Prepare digital and data awareness essentials for leadership,
- Raise decision-makers' awareness of digital technologies through formal workshops and
- Include digital awareness in debates and conversations organised by the Prime Minister's Office.

Outcomes:

- Accelerated support to digital government by leadership (Prime Minister, the Council of Ministers and leadership of Ministries, Departments, Agencies, regional and local government) and
- Increased leadership's awareness of data and digital government.

14.2 Increase the Leadership Role of the Digital Transformation Council in Digital Government

The Digital Transformation Council, established legally in 2024, is a critical tool for the success of digital government because it provides oversight on implementing the Digital Ethiopia project in general and this Digital Government Strategy in particular. The Council can resolve implementation issues and facilitate inter-agency collaboration and planning. The Digital Transformation Council will:

- Provide overall political and technical leadership in digital government development activities, priorities and direction,
- Act as a convener of the highest-level officials of digital government stakeholder entities, including the private sector and development partners,
- Review digital government priorities, Initiatives and Interventions,
- Review implementation reports and consider the progress of digital government implementation and emerging issues,
- Ensure a whole-of-government approach other than individual MDA efforts,
- Advocate for mobilising resources to support the implementation of Digital Government Strategy.

The Strategy proposes increasing the Digital Transformation Council's leadership role in implementing the Digital Government Strategy.

DGEN 2 – Increase the Leadership Role of the Digital Transformation Council in Digital Government

Actions:

- Appraise the Digital Transformation Council with different aspects of the digital government strategy and its implementation roadmap.
- Increase the Digital Transformation Council's role in implementing a Digital Government Strategy that prioritizes technology, people engagement and processes.

Outcomes:

- Increased awareness of digital government,
- Increased coordination of the implementation of digital government.

14.3 Thematic Technical Committee(s) on Digital Government

The Digital Transformation Council is expected to include individuals from different public sector institutions appointed by the Prime Minister to set strategic directions. The Council will need technical advice from sectoral and technical experts on different aspects of digital government. Therefore, given the size of the Ethiopian state, and in line with the envisaged whole-of-government approaches, it is recommended that up to six thematic technical advisory committees on digital government development support the Council. The Technical Committees (TCs) will be dedicated to the implementation of their thematic interventions defined in the strategy and reports their plans and accomplishments to the Council.

The Technical Committees, which will draw from domain/sector experts and leading experts in digital government in Ethiopia and abroad coming from universities and the private and public sectors, will provide expert services, including:

- Advise the Digital Transformation Council on trends and practices of digital government,
- Conduct an independent review of progress in the implementation of digital government strategy and forward it for review by the Digital Transformation Council,
- Support the Digital Transformation Council in the mobilization of technical and financial resources for digital government,
- Review the e-Government Development Strategy initiatives, programmes, interventions, projects and actions defined under their pillars
- Propose as appropriate new e-Government Development initiatives, programmes, interventions projects and actions defined under their pillar. Reviewing any new interventions concept notes and making recommendations Council
- Create implementation focused project Technical Working Groups to implement e-Government Development initiatives, programmes , interventions under their pillars.
- Monitor implementation of e-Government Development strategy initiatives, programmes, interventions, projects and actions the based on the e-Government Development Strategy objectives, key outputs, indicators and performance targets in the results framework.
- Support the Technical Working Groups in the resolution of constraints and impediments to implementation of activities in the cluster.
- Conduct broad stakeholder technical consultation on key issues and harmonising MDA, regional and local government and stakeholders' plans and positions,

The GoE will establish the following technical committees for digital government to support the Digital Transformation Council on technical matters.

Figure 20: Proposed Initial 6 Technical Committees

DGEN 3 – Establish Sectoral Technical Committees on Digital Government

Actions:

- Identify members of the technical committees based on merits and willingness to contribute to the digital government
- Formally appoint the members of the Technical Committees on Digital Government,
- Support the work of the Technical Committee on Digital Government

Outcomes:

- Availability of a Technical Committees to support decision-making and implementation of digital government.
- Enhanced implementation of digital government strategy based on practice, insight and data.
- Increase sharing of knowledge on digital government topics.

14.4 Advance the Coordination Role of the Ministry of Innovation and Technology

The Ministry of Innovation and Technology, as leader of the digital development sector, is responsible for the overall coordination of implementing the Digital Government Strategy. The MInT will play the following role in the implementation of this Strategy:

- Hosting the Digital Government Service Centre,
- Acting as Secretariat to provide technical and administrative support and coordination to Digital Transformation Council and Technical Committees activities, and manage meetings and action logs using Standard Operating Procedures
- Building a digital government development community by ensuring national buy-in, collaboration and full ownership of all stakeholders' strategy interventions and activities. This includes interaction and information sharing on digital government across MDAs, regional governments and local governments,
- Promoting cooperation, learning and synergies within and between Technical Committees activities,
- Reviewing the Digital Government Strategy objectives and interventions, schemes and time-bound programs and projects, as desired,
- Coordinating the preparation of the Detailed Implementation Action Plans (DIAPs) and project TORs for the Digital Government Applications and Services, Digital Government Foundation, and Digital Government Enabler projects.
- Leading in the coordination of the implementation of national-level interventions and dialogues,
- Producing an annual Calendar for all Digital Government Development scheduled meetings and events for the Digital Transformation Council and Technical Committees and Working Groups,
- Reporting to various bodies, including the Digital Transformation Council, the Council of Ministers, and the Prime Minister, on the progress of digital government.

Country experiences show that leadership in digital government will require both mandate and technical competency to drive digital transformation in the public sector. Therefore, the MInT must build all the necessary capacity to provide these services and incentives to attract and retain talent.

Experience like the one in Mauritius also shows that institutions responsible for the development of digital technologies, such as INSA, AI Institute, MInT and regional ICT agencies, need to coordinate and cooperate, first by focusing on their core mandates, like cyber security and the integration of emerging technologies in development, policy, programmes and execution.

DGEN 4- Advance the Coordination Role of the Ministry of Innovation and Technology

Actions:

- Increase the number of digital government management staff at MInT,
- Develop the capacity of MInT staff in different topics of digital government and
- Provide incentives and career paths for the staff.

Outcomes:

- Improved capacity of MInT to oversee digital government projects, producing annual calendars and reporting to different bodies,
- Enhanced capacity of MInT to develop policies, guidelines and standards on digital government and
- Enhanced MInT's IT capacity to coordinate with MDAs, regional government and all other players to create a digital government community within the framework of a whole-of-government approach.

14.5 Establish and Operationalise a Digital Government Support Centre

The Digital Government Support Centre, discussed in APS 1 above, will be an important arm of the government that will manage digital government projects, assess progress and adherence to the relevant digital government guidelines and standards, and prepare annual reports on digital transformation for review by the Digital Transformation Council and Digital Government Technical Committees. The DGSC provides a wide range of roles, including:

- Supporting and maintaining shared citizens and business portals,
- Provision of IT services and advice to MDAs, regional and local governments and supporting those who do not have the necessary in-house capacity in their digitalization effort through both expertise (ad-hoc guidance, templates, documentation, etc.) and technical components (SaaS, PaaS, IaaS, etc.)
- Building and supporting common platforms, services, components, and tools,
- Maintaining sharable and reusable applications and resources,
- Foster collaboration between public sector and private sector innovators,
- Supporting different entities in developing and executing an eServices implementation based on users and business journey perspectives and their integration based on the GovStack platform and “EthioConnect” enterprise bus service. The plan will also cover how a particular MDA, as well as regional and local governments, applies omni-channels to deliver the services.
- Devising and enforcing minimum standards to be applied consistently across Government digital services based on GEA and interoperability framework to ensure compatibility among the several systems in use in the public sector,
- Hosting a forum for IT managers in the public sector to discuss ICT issues and to provide feedback on IT initiatives/issues to the central agency and

- Participation in skills development.

DGSC will be staffed with highly skilled technical staff to meet the growing digital government requirements. The staff will have appropriate incentives to drive digital government.

14.6 Establish Platform for Cross-Government Coordination

Currently, there is a limited platform for coordination between the MInT and Ministries, Departments and Agencies, and regional and local government on the digitalisation of public services. Ad hoc coordination is being done individually through MInT, the Artificial Intelligence Institute of the Information Network Security Agency. Establishing a formal cross-governmental coordination structure is important to ensure the whole-of-government aspect, bringing key stakeholders together through forums and committees with a coordination or collaboration remit. A platform that brings all MDAs' IT departments and other key players together to discuss digital public service issues, share practice components, and support interoperable government is crucial. The platform, which combines bi-annual face-to-face meetings and an online portal, will be useful to ensure:

- Discussion of challenges and opportunities in digital government,
- Hosting tutorials, training workshops and boot camps on different aspects of digital government to upgrade skills,
- Discuss strategies, designs, sharable applications and components,
- Provide incentives for excellence in digital public services (e.g., annual awards in innovative digital public service)
- Integrating change management and communication plans in all digital government initiatives,
- Draw on GEA as a coordination and standards enforcement tool,

To participate in the platform, MDAs, regional and local governments need to appoint a Chief Information Officer (CIO) or senior digital and data development offices (CDOs), Security Officers (SOs), or technology officers in charge of their networks (CTOs), which could convene and make important strategic decisions concerning the rapid acceleration of digital services.

DGEN 5- Create a Platform for Cross-Government Coordination on Digital Public Service

Actions:

- Encourage MDAs and regional and local governments to assign CIOs, CTOs, SOs, CDOs,
- Establish a face-to-face and virtual platform for CIOs, CTOs, SOs and CDOs,
- Sustainably support the forum.

Outcomes:

- Availability of face-to-face and virtual platforms for coordination on digital government between MDAs, regional and local governments,
- Improved coordination of digital government,
- Enhanced capacities of CIOs, CTOs, SOs and CDOs, and

Increased standardisation and data sharing.

14.7 Support the Establishment of Project Technical Working Groups on Digital Government Topics

Due to the wide range of activities under each e-Government Development Strategy objectives and the large number of involved stakeholders, implementation focused Technical Working Groups (TWGs) shall be created by the Technical Committees to broaden ownership and provide project specific implementing platforms to consider , in a more comprehensive way, the project actions listed in the strategy and implement them. The life of a TWG is therefore tied to that of an intervention or project, or otherwise as decided by the parent technical committee.

This will allow the TCs to limit their discussion to strategic planning issues of the interventions while at the same time ensuring adequate attention is given to the detail for each intervention action within the TWG. Membership to each TWG shall also continue to be cross-institutional, and shall include, where necessary, external partners (Development Partners and Private Sector technocrats) to engender detailed technical dialogue and implementations The Mint or Digital Government Support Centre may modify the number and composition of the working groups.

Specific functions for each Working Group shall be as follows:

- Comprehensive review and fleshing of Strategy actions, timelines, human resources and budgets.
- Ensuing harmony between DIAPs in implementation across other Strategy clusters
- Monitoring the implementation of the thematic sections of the DIAP and raising issues for TCs consideration,
- Collecting and collating the DIAP actions quantitative and qualitative progress results
- Reviewing and clearing thematic sections of the Annual and semi-annual performance reports before consideration by the TCs,
- Reviewing new interventions concept notes and making recommendations to TCs for clearance
- Any other assignments as needed by the TCs

The head of the lead MDA will be the committee's chairperson. The Digital Government Support Centre will be the secretary for each of the Working Groups. The Working Groups will establish proper meeting records, strict follow-up and evaluation to meet joint plans and agreements and ensure accountability for failures and recognition for successes. A

result-reporting framework will guide the Working Groups. They will prepare annual progress reports on defined interventions and actions and submit a consolidated annual report to the Digital Government Support Centre.

DGEN 6 –Support Technical Committees in Creating Technical Working Groups

Actions:

- Assist Technical Committees in creating TWGs
- Help Identify lead MDAs,
- Establish operating procedures, including result reporting framework,
- Support the work of the Technical Working Group sustainably.

Outcomes:

- Availability and operation of Technical Working Groups on different projects of digital government
- Improved technical discussion on digital government
- Enhanced implementation of the digital government strategy,

15 Digital Literacy, Skills and Culture for Government Workforce and Users

Digital literacy, skills, and civil service innovation culture to support citizens and businesses in a digitalised online environment are rated as the critical ingredients for successful digital government. The situation analysis indicates core digital skills are generally absent at MDAs' regional and local governments. The level of information and digital literacy is also low across the population.

Digital skills are increasingly becoming the most critical component of individual competency, whether someone is working in the public or the private sector. Twenty-first-century jobs also demand problem-solving, communication and collaboration, entrepreneurial spirit, and the ability to use digital technologies for work and life. Basic digital literacy is helpful, but most jobs today require intermediate and advanced skills. The range of digital skills required for digital government includes:

i. Basic digital literacy necessary for day-to-day work (e.g., access to online information or pay for services),
ii. Digital literacy for all types of jobs, especially those that can be gained at TVET and college levels whose graduates must be literate in using technology to do day-to-day jobs, like using platforms to deliver services for citizens and businesses,
iii. Digital proficiency in specialised jobs like health, education, agriculture, etc. In health, government staff are expected to use data for health decision-making. In education, teachers are required to use e-learning tools to conduct blended face-to-face and online learning,
iv. Advanced skills in design and development of digital technologies (e.g., software development, big-data analytics, networking, web design and digital technology project management skills),
v. New and emerging technologies skills (e.g., IoT, Artificial Intelligence, blockchain, cloud computing, big data analytics); and

Table 8 summarises the different categories of pertinent digital and related soft skills identified by different international organisations.

Table 8: Different Categorisation of Digital Skills

Institution	Categorisation of Digital Skills Requirement
International Telecommunications Union[16]	• Advanced digital skills (coding and other algorithmic knowledge) • Basic digital skills (related to the use of technologies) • Soft skills (such as communication and leadership) • Digital entrepreneurship (online market research and using financial platforms)
World Economic Forum[17]	• Abilities (cognitive and physical) • Basic skills (content and processing skills) • Cross-functional skills (social systems, complex problem solving, resource management and technical skills)
Organisation for Economic Cooperation and Development[18]	• Technical and professional skills (specific and often industry-specific skills such as installation and operation of machines) • Generic ICT skills (skills needed to understand, use and adapt technologies; life-learning ability to adapt to technology changes) • Complementary ICT soft skills (creativity, communication skills, critical and logical thinking, teamwork, digital entrepreneurship)

The Government of Ethiopia realises that these skills are essential for economic growth. The national digital skills framework for TVETs and higher education advocates for (1) establishing enabling policies, digital skills framework, and digital skills assessment; (2) reform of digital skills programs; (3) enhancing the use of technology in teaching-learning; (4) connect higher education and TVET institutions to affordable high-speed broadband; and (5) capacity building and process reengineering in ministries.

[16] ITU Digital Skills Toolkit, https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf

[17] World Economic Forum, 2016. The future of jobs: Employment, skills and workforce strategy for the fourth industrial revolution. In Global challenge insight report. Geneva: World Economic Forum.

[18] OECD, 2016. Skills for a digital world: 2016 ministerial meeting on the digital economy background report. OECD Digital Economy Papers

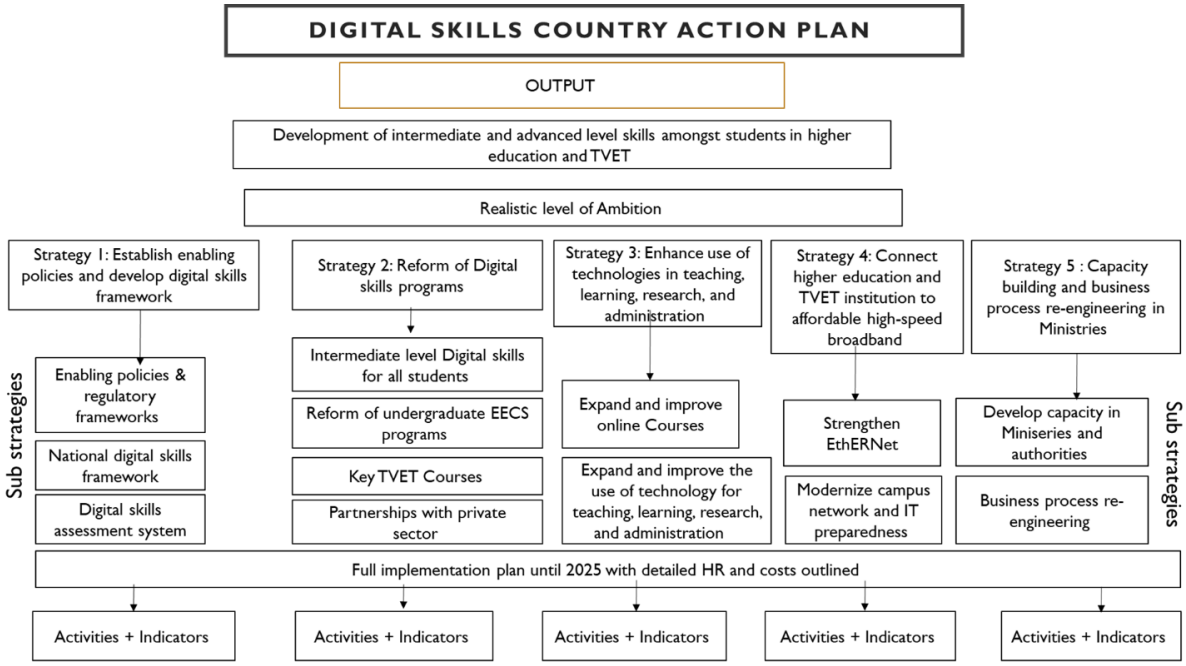

Figure 21: National Digital Skill Action Plan

The development of digital government human capital will begin with creating digitally confident leaders and civil servants in government who can adopt digital technology for the design, use, and management of systems in response to the needs of the people. Based on the national digital skills framework and experience of different countries, the GoE will:

i. Develop civil servants' digital competencies – literacy, skills and digital-driven service culture.
ii. Provide digital literacy training for decision-makers,
iii. Build digital skills for those working on digital government projects or Information Technology Departments at MDAs, Regional and Local Governments,
iv. Increase the supply of digitally skilled workforce,
v. Increase public digital literacy.

15.1 Accelerate Digital Literacy and Skills for Civil Servants

The civil service needs essential digital skills to effectively use digital technology and enhanced or specialised digital skills to work in roles significantly impacted by these technologies (e.g., human, financial and education management systems—IFMIS, EMIS, HMIS, etc.). They also need character traits, know-how, and work habits to support clients in a digitalized environment.

The design of government staff skills will begin with the assessment of the competency of civil servants to identify reskilling opportunities. The GoE will conduct a competency assessment of the skills of its workforce to formulate a comprehensive plan for digital literacy and skills. It will evaluate and adopt digital competency frameworks like the UNESCO Global Framework of Reference on Digital Literacy Skills, the European Commission DigComp framework, and the Digital Intelligence (DQ) framework. Drawing on these frameworks, the government will develop a national digital competence framework that sets out the standards for the qualification and national workforce plan, national career framework, and gender equality program to foster equal participation of men and women in delivering digital-enabled public services.

Source: European Union, The Digital Competence Framework for Citizens With new examples of knowledge, skills and attitudes, 2022

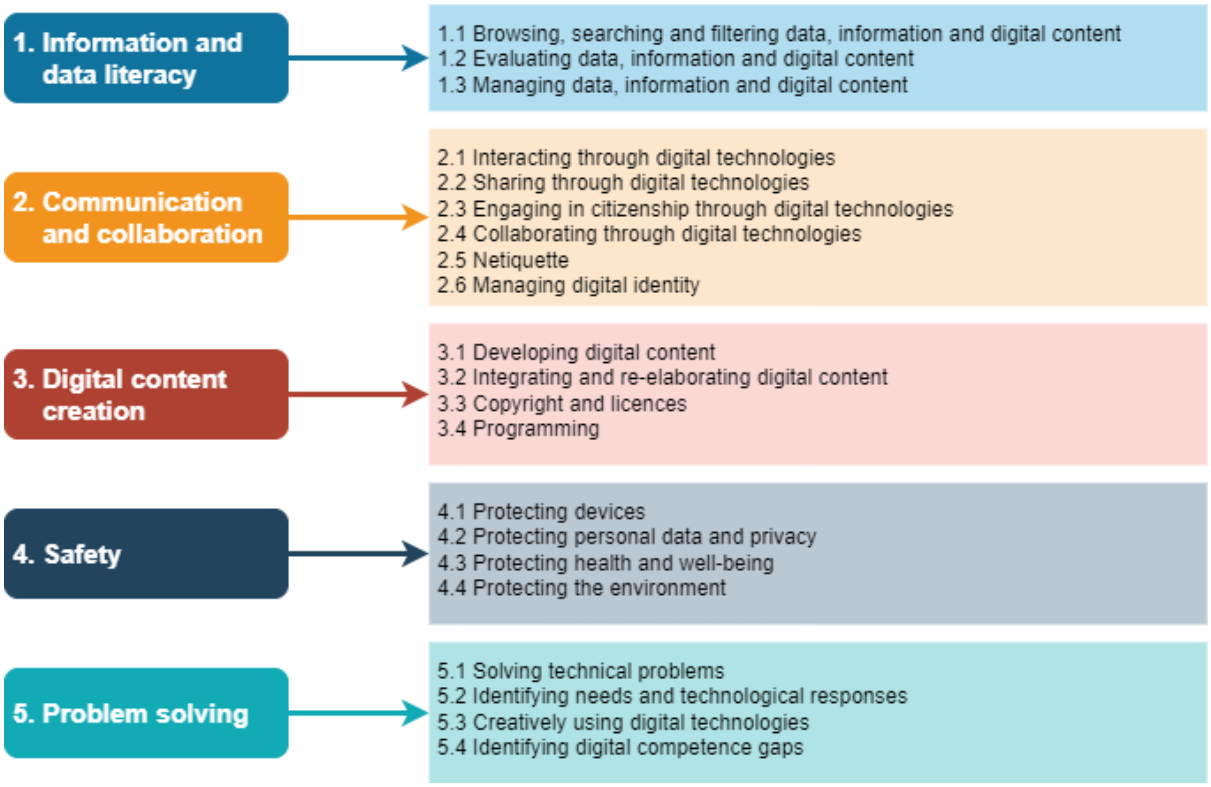

Figure 22: DigiComp Conceptual Reference Model

To strengthen the digital skills of its workforce, the GoE will conduct regular ICT training, seminars and learning sessions for civil servants and adopt a conducive recruitment and retention strategy that promotes digitally-enabled public service delivery. It will modernise human resources management to support civil service staff's attraction, recruitment, development, and retention. Retention of the skilled ICT staff is a key challenge that will be addressed by introducing competitive salary packages, career development programs, and collaboration with universities for ongoing skill development.

The Digital Government Services Centre will design a series of courses based on staff members of MDAs and regional and local governments and serve as a digital academy

for delivering skills in digital government. This training will focus on the deep technical skills the government staff must undertake in specific transformation projects. The GoE will also work closely with the academic institutions and private sector to deliver a series of training courses.

DGEN 7 – Develop Government Staff's Digital Competencies – Literacy, Skills and Digital-driven Service

Actions:

- Conduct a competency assessment of the skills of its workforce to formulate a comprehensive plan for digital literacy and skills,
- Evaluate and adopt digital competency frameworks,
- Conduct regular ICT training, seminars and learning sessions for civil servants and
- Modernize human resources management to support civil service staff's attraction, recruitment, development, and retention.

Outcomes:

- Improved government staff competencies - literacy, skills and digital-driven service culture for effective public service delivery,
- Enhanced retention of skilled government staff.

15.2 Digital Literacy for Leadership

Due to their competing priorities, decision-makers often have limited time to spare on digital technology issues. However, there is a need to bring all decision-makers closer to the realities of digital government services. Leadership should understand not only the opportunities but also the challenges, including the implications of emerging technologies. It is thus critical to deliver tailored training for leaders at ministries, agencies, and regional and local governments to improve their understanding of technologies, solutions, and the people and process issues affecting digital public service delivery. The Digital Government Support Centre will prepare a data and digital government curriculum tailored to different decision-makers contexts and deliver short-term training.

DGEN 8 - Provide Digital Literacy Training for Decision-makers

Actions:

- Develop a data and digital government curriculum for decision-makers and
- Deliver data and digital literacy for decision-makers regularly.

Outcomes:

- Increased awareness of decision-makers on data and digital government issues and
- Enhanced support for digital government.

15.3 Develop Competency of MDA, Regional and Local Government IT Professional Staff

The digital skills of professional staff in the government information technology department are a key stumbling block to developing a digital government in Ethiopia. Chief information officers at MDAs and regional governments indicate that their primary challenge was finding skilled staff and the turnover of the ICT workforce. They face significant problems in attracting skilled resources to perform ICT-related tasks due to the limited pool of skilled candidates and the government's inability to match salaries to that of the private sector. It was noted that colleges and universities are not producing the desired digitally-ready workforce.

A critical skill shortage area is open-source software, which is critical for designing digital public goods[19] and infrastructures[20] and driving digital government using the building blocks approach and their technical specifications. Ethiopia's open-source community is insignificant and cannot support open-source technology-based applications and services critical for modern digital government. Other areas of digital skills shortage cited by the stakeholders include:

- Application development and testing,
- Enterprise architecture,
- User interface design – including multi-channel applications,
- Internetworking and server administration - switching, routing, network security, server administration,
- Database design and management – SQL, MYSQL, Postgres, database administration, data analytics,
- Emerging technologies –cloud computing, artificial intelligence, blockchain, IoT, big data analytics,
- Web services, Microservices, REST/SOAP APIs, cloud deployment, container deployment, developing and deploying containerized applications, and
- Internet security.

There is also a need for DevOps specialists, Graphic design specialists, Software Developers, Software Quality Testing (SQT) Automation specialists, Web Programming

[19] Digital Public Goods within the context of digital government include open-source software, open data, open AI models, open standards, and open content that adhere to privacy and other applicable laws and best practices, do no harm by design, and help attain the development goals.

[20] Digital Public Infrastructure within the context of digital government include digital forms of ID and verification, civil registration, payment (digital transactions and money transfers), data exchange, and information systems (including sector-specific, i.e., health or education).

specialists, and System auditors, among others. Ethiopia lacks a critical mass of experts with open-source software skills. However, it is imperative that the GoE and universities encourage open-source software-based innovation, which will be beneficial in the long term from cost and application quality perspectives.

The Government of Ethiopia will put different mechanisms in place to develop skills of the ICT workforce at MDAs, including hub and accelerators-based training, boot camps, tutorials, workshops and coding challenges. It will pursue on-the-job assignments, online learning, peer learning, and participation in conferences as a mechanism for upgrading digital skills. Digital skills will also be supported with improved incentives for skilled staff. Placing senior staff on contract would allow for greater remuneration flexibility, and implementing an effective reward system based on performance will be considered to ensure those working in this dynamic field dedicate their time and resources to improved digital government.

DGEN 9 – Build Digital Skills for those Working on Digital Government Projects or Information Technology Departments at MDAs, Regional and Local Governments

Actions:

- Use hub and accelerators-based training, boot camps, tutorials, workshops and coding challenges for building skills for government professional staff,
- Modernize human resource management and remuneration for the digital technology staff to attract, recruit and retain talent

Outcomes:

- Accelerated skills for IT professional staff at MDAs, regional and local government that enhance digital public service planning and implementation,
- Improved retention of skilled government professional staff

15.4 Increasing the Supply of Skilled Workforce

The supply of digital skills, particularly for advanced and highly specialized skills, relies on a pipeline of qualified graduates. Therefore, an improved secondary and tertiary education curriculum and a long-term digital education master plan will be critical. The Government will improve ICT, Internet and digital government education across primary, secondary and tertiary levels. It will encourage youth, especially young women, to uptake digital skills and major in fields related to digital technology to reduce the gender gap. It will improve digital technology labs and teacher training.

Digital government is not a key topic of universities at the moment; therefore, there is a need to integrate digital government-related courses in higher education to meet the growing professional requirements, especially within the context of the 4th Industrial Revolution. This includes courses on enterprise architecture and usable components,

advanced internetworking, artificial intelligence, blockchain, data science, and digital security. Universities must also upgrade their curriculum and practice to train students to use the latest tools to solve digital government challenges.[21] The GoE will also support research and development programs in universities in the various digital government fields and foster "triple helix" collaboration between academia and public and private sectors to develop digital government solutions.

DGEN 10 – Increase the Supply of Digital Skilled Workforce

Actions:

- Reform curriculum in TVETs and colleges to train graduates on digital government topics,
- Support research and development programs in universities in the various digital government fields.
- Incorporate incentives for skill retention, such as career advancement for IT professionals in government roles.
- Integrate coding in primary and secondary schools education curriculum to create a better digitally skilled future generation.

Outcomes:

- Increased supply of digitally skilled graduates,
- Improved research and development on digital government topics.

15.5 Digital Service Awareness and Literacy for Citizens and Business

Finally, increasing citizens' and businesses' awareness of e-services is essential. Digital literacy for digital government should focus on a wider group of the population, including marginalised people like youth, women, older people, and people with disabilities, as well as those who need the services the most benefit from digital technologies and digital public services. This can be achieved through a dedicated awareness-raising programme that helps people become good users of Internet services, including public e-services. The Government will organise talk shows, radio and TV programmes, awareness weeks, etc. The Government will draw on the well-developed Information, Education and Communication (IEC) campaigns used in other fields, like the health sector, to design

[21] Contemporary core technology skills cover mastering phyton, java, rust, mobile development using Swift and Kotlin, version control using Git, mastery of cloud platforms like AWS, Azure, and GCP, machine learning fundamental using R and TensorFlow, cross-platform mobile apps development frameworks such as Flutter, reach Native and Xamarin, mastery of DevOps tools – Github, bitbucket, Jenkins or Bamboo, understanding of blockchain development environment and WebAssembly.

digital government awareness programmes for citizens. It will work with stakeholders such as civil society, media institutions and local authorities.

DGEN 11 – Increase Public Digital Literacy

Actions:

- Leverage community centres, CSOs and media to organise public digital literacy, and
- Use information communication techniques like talk shows, radio and TV programmes, and awareness weeks to raise the digital awareness of the public.
- Increase Grassroots Engagement: training rural citizens through community-based programs.

Outcomes:

- Improved collaboration between government, CSO and media on raising public awareness of digital technologies and digital government and
- Enhanced awareness about digital services by citizens and businesses.

16 Advancing Legislation for Digital Government

A legal and regulatory environment is essential for promoting certainty and confidence in using digital public services to protect the rights and security of citizens and businesses within and outside the public sector. A wide range of laws and regulations facilitate digital public service. The main legal, policy and regulatory instruments include:

- There are laws on data privacy, consumer protection, digital signatures, digital identification, cybersecurity, e-commerce and public-private partnerships.
- Laws governing institutional mandates and arrangements are also important because they help delineate the roles and responsibilities in data management, sharing and use, e-government coordination and other aspects such as security and privacy enforcement.
- Public-Private-Partnership law encourages private sector participation in digital development and sharing its knowledge and expertise with the public sector, contributing, in the long term, to balanced economic growth.

Some guidelines and directives are used in digital government and enterprise architecture principles like digital-by default, security-by-design, privacy-by-default, open-by-default, cloud-first and mobile-first principles. Many governments also design policies, legislation, and strategies to address emerging technology issues.

The Government has promulgated three legislations to facilitate trust in electronic government –

- The Electronic Transaction Proclamation No. 1205/2020 recognises the validity and enforceability of e-contracts under the functional equivalence approach, which presupposes the existence of equivalent conventional contract rules.
- The Electronic Signature Proclamation No. 1072/2018 recognises electronic signatures, facilitating their acceptance in online messaging and transactions.
- Computer Crime Proclamation No. 958/2016 is intended to provide authorities with the "legal mechanisms and procedures to prevent, control, investigate and prosecute computer crimes and facilitate the collection of electronic evidence".
- The Personal Data Protection Proclamation (Proclamation No. 1321/2024) establishes a robust legal framework for data protection in Ethiopia.

While these laws provide the basis of electronic contracts, digital signatures, and the prevention of cybercrimes, they need to be reviewed and supported by different guidelines to meet the consumers' needs in line with growing threats and emerging issues of privacy and security. An effort to develop a data protection law that outlines data legitimacy, data minimization, accuracy storage, security, etc., is underway. Still, the law needs to be enacted by the parliament. In sum, key gaps remain in legislation in the following areas:

- Develop core guidelines for the implementation of the Personal Data Protection Law.
- Amend and combine current trust and digital ID laws to form a comprehensive digital identification and trust law covering the aspects of digital identification, digital signature, electronic documents and electronic contracts,
- Revised cyberlaw considering recent global developments in cyber threats include, for example, unauthorized access to computer systems, unauthorized monitoring of data, unauthorized alteration of data, unauthorized interference with computer systems, content-related offences, financial crimes and cyberstalking,
- Adopt a law providing for open access to government information,
- Adopt instruments for promoting digital government, interoperability and enterprise architecture principles,
- Develop legislation on emerging technologies in society and government (blockchain, AI, data analytics, IoT, green technologies).

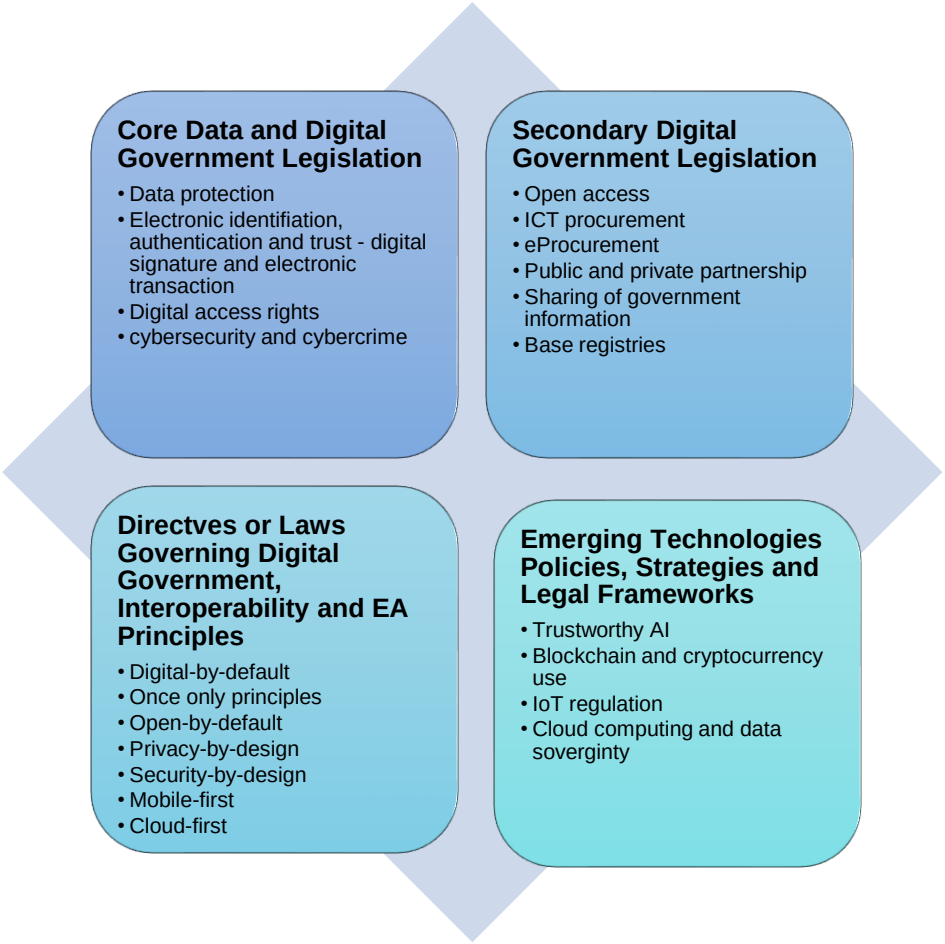

Figure 23: Main Legislation and Guidelines for Digital Government

The GoE will assess existing legal and regulatory instruments for digital government. It will keep the legislation up to date to seize opportunities and tackle challenges posed by digital reforms, taking the advances in the last decades' country and regional experience

in establishing legal and regulatory frameworks that facilitate inter-government coordination and data sharing.

16.1 Developing Guidelines and Tools for Implementation of Personal Data Protection in the Public Sector

The enactment of the Personal Data Protection Law needs to be accompanied by the necessary guidelines, tools, and strategies to operationalise the law. These range from conducting personal data and special categories of data to be protected, developing various consent forms for different organisations and personal data managers, putting compliance mechanisms in place and drafting related guidelines on privacy, data storage and sovereignty and treatment of non-personal data.

DGEN 12 – Develop the Necessary Guidelines and Tools for the Operationalisation of the Data Protection Law within the Public Sector

Actions:

- Identify core guidelines that promote compliance with the data protection law in the public sector
- Conduct public consultation on different guidelines and compliance tools in the public sector
- Ensure compliance with data protection law provisions in the public sector.

Outcomes:

- Availability of data protection implementation instruments and

Increased trust in government services through enhanced data protection

16.2 Amending the Electronic Transaction, Digital Identity and Digital Signature Laws and Adopting Comprehensive Digital Identification and Trust Law

The current e-transaction and digital signature laws need amendments to include digital identity and other aspects of trust in line with global experiences. Creating an electronic identity and trust law will bring all the different laws, such as e-transaction law and digital signature law, and digital identity law. While Digital Identity Proclamation No. 1284[22] provides an overall legal framework for digital identity, a single framework for electronic

[22] https://drive.google.com/file/d/19tuJhXg8VIblV4-ZpEF9jPf6h8vT6gjd/preview

identification (eID) and trust services, including electronic signature, electronic seal, electronic time stamp and electronic transaction services, will be useful for comprehensive legislation for digital trust. The Government will initiate a process of revising current laws in trust areas, engage with stakeholders by launching a consultation process, and provide capacity building and activities that take the new laws through the legislative process.

DGEN 13 – Amend and Combine Current Trust and Digital ID Laws to form a Comprehensive Digital Identification and Trust Law

Actions:

- Review the adequacy of the current digital signature, digital ID and electronic transaction laws,
- Conduct public consultation on desired modifications, and
- Amend or combine current trust and digital ID laws to form a comprehensive digital identification and trust law covering the aspects of digital identification, digital signature, electronic documents and electronic contracts.

Outcomes:

- Increased trust in government services through enhanced electronic trust, identification and digital signature laws.

16.3 Revision of Cybercrime Law

The GoE realises that while the Computer Crime Proclamation No. 958/2016 provide the basis for prosecuting offenders of cybercrime, it does not provide all the codes needed to address cyber-dependent crimes (i.e., "any crime that is committed using computers, computer networks or other forms of information communication technology;" and cyber-enabled crimes (i.e., traditional crimes facilitated by the Internet and digital technologies). There has been significant growth in cyber-enabled crimes in the last decade; thus, laws should be strong to address this trend. The government will review Computer Crime Proclamation No. 958/2016 to assess its suitability in addressing growing cybercrime and amending the relevant codes to meet challenges in this area.

DGEN 14 – Revise Cyberlaw Considering Global Developments in Cyber Threats

Actions:

- Assess the suitability of the current computer crime proclamation to address growing cyber threats,
- Revise cyberlaw considering recent global developments,
- Conduct public consultation, and
- Adopt cyberlaw.

Outcomes:

- Increased trust in government services through new cyber laws and
- Increased capacity to prosecute cyber threats.

16.4 Adoption of Law Providing for Open Data

Open Data is an important aspect of digital government that provides the public access to information in various formats. Increasing access to available government data improves transparency and accountability within government, supports evidence-based policy development and provides a platform for innovation. The government will establish a law that encourages the proactive public release of government information by MDAs and regional and local governments in ways that respect data sharing and privacy safeguards. The law on open access will improve the sharing, use and reuse of public-sector data, encourage private-sector innovation, and make citizens and government more consultative, participative and accountable. The GoE will:

- Review progress in opening data by MDAs, regional and local government,
- Assess laws and policies governing open data,
- Establish an open data access law,
- Adopt open data law through public consultation,
- Create instruments to encourage the availability of open data and
- Ensure that data is used for transparency, evidence-based policymaking and innovation.

DGEN 15- Adopt a Law Providing for Open Data

Actions:

- Review current guidelines and laws that promote open data,
- Develop open access law,
- Adopt the law through public consultation and
- Establish instruments to encourage the use of open data.

Outcomes:

- Increase access to open government data, and
- Improved innovation and decision-making.

16.5 Adoption of Directives Promoting Digital Government, Interoperability and Enterprise Architecture Principles

Digital government is built on principles such as digital-by-default, once-only, data-by-default, privacy-by-design, security-by-design, mobile-first, and loud-first approaches. These principles need to be enforced either via a law or directives of the Council of Ministers:

- Digital-by-default aims to establish digital communication as a primary method while utilizing traditional channels for those who do not have access to the Internet, do not have the relevant skills, or are in a unique situation requiring specific assistance.
- The mobile-first strategy ensures that digital services are adapted to be available via mobile phones.
- The once-only principle ensures that citizens and businesses only have to provide certain information to the government authorities once (also known as a "Tell us Once Principle") without requesting or requiring them to submit the same data multiple times. This principle reduces the entry of inconsistent data, administrative costs, and the workload of competent authorities and stakeholders in collecting, storing, and using data.
- The cloud-first approach promotes the adoption of cloud technologies for all new applications, platforms and infrastructure. It is a strategy that prioritizes cloud computing services over legacy IT systems.
- Privacy-by-design – is an approach Privacy for proactively embedding privacy into information technology, business practices, and networked infrastructures. The Privacy by Design measures are designed to anticipate and prevent privacy-invasive events before they occur.
- Security-by-design emphasizes technology products, including hardware, software and networks, to be designed and built to reasonably protect against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure. It also promotes the approach that applications should be launched following risk assessment to identify and enumerate prevalent cyber threats to critical systems and then include protections in product blueprints that account for the evolving cyber threat landscape.

These and other principles, including common technological standards for digital platforms, web services, API standards and catalogues and digital service delivery standards, must be adhered to across government and outlined in directives and laws to ensure compliance. Country experiences indicate these principles are mandated through legislative and government directives. The GoE will:

- Assess the application of key digital government, interoperability and enterprise architecture principles using different mandates (directives, laws, regulations, guidelines),
- Assess the suitability of different instruments (guidelines, directives or laws)
- Consult with stakeholders on the implementation of digital government, interoperability and enterprise architecture principles,
- Create the necessary instruments like the Council of Minister Directive to enforce digital government principles such as digital-by-default, once only, open-by-default, privacy-by-design, security-by-design, mobile-first, cloud-first)

DGEN 16 - Adoption of Directives Promoting Digital Government, Interoperability and Enterprise Architecture Principles

Actions:

- Assess the application of key digital government, interoperability and enterprise architecture principles using different mandates (directives, laws, regulations, guidelines),
- Assess the suitability of different instruments (guidelines, directives or laws),
- Consult with stakeholders on the implementation of digital government, interoperability and enterprise architecture principles and
- Create the necessary instruments like the Council of Minister Directive to enforce digital government principles such as digital-by-default, once-only, open-by-default, privacy-by-design, security-by-design, mobile-first, and cloud-first).

Outcomes:

- Increased trust in government services through enhanced principles such as digital-by-default, once only, open-by-default, privacy -by-design, security-by-design, mobile-first, cloud-first,
- Enhanced availability of shared services.

16.6 Adoption of Policies and Strategies Promoting Different Uses of Emerging Technologies in Society and Government

Integrating emerging technology in public services and the economy demands a comprehensive strategic process that assesses their adoption opportunities, challenges and ethical issues. The GoE will prioritise strategies and regulations that advance AI, blockchain, data analytics and IoT. The Government will:

- Develop laws, regulations and ethical norms that promote AI application in the economy and the public sector to address economic, ethical, policy and legal implications of using artificial intelligence and machine learning.

- Initiate a comprehensive policy and strategy on blockchain technology through dialogue with all stakeholders on the potential use of blockchain technology in government and the economy.
- Establish guidelines on big data analytics that identify available data sources, assess the current state of data usage in government, and encourage big data use cases to improve the effectiveness and efficiency of the public sector.
- Promote enabling regulatory regimes on security, privacy, and intellectual property, as well as transparent and predictable market access regimes for IoTs. ETA should be ready and equipped to address concerns about privacy, security, quality, spectrum, and IoT standardisation.

DGEN 17 – Adoption of Policies and Strategies Promoting Different Uses of Emerging Technologies

Actions:

- Develop laws, regulations and ethical norms that promote AI application in the economy and the public sector,
- Initiate a comprehensive policy and strategy on blockchain technology through dialogue with all stakeholders,
- Establish guidelines on big data analytics and
- Promote enabling regulatory regimes on security, privacy, and intellectual property, as well as transparent and predictable market access regimes for IoTs.

Outcomes:

- Availability of emerging technology laws, guidelines and regulations, and
- Accelerated use of emerging technologies for digital public services.

16.7 Development of Green Digital and Electronic Waste Policy and Legal framework

Associated with the increasing digitisation of the Ethiopian government, economy and society as a whole is the rapidly increasing generation of waste electronic and electrical equipment (WEEE), commonly referred to as e-Waste. There is currently no identifiable policy or legal framework to guide the management or control of electronic waste. In line with the stated strategy objective of promoting eco-friendly practices in digital government operations and reducing electronic waste, the GoE will prioritise the development and coordination of strategies and regulations regarding managing. The Government will:

• Develop laws, regulations and ethical norms to guide environmentally sound disposal and recycling of Waste Electrical and Electronic Equipment

• Develop laws, regulations and ethical norms that promote Green Digital technology deployments

universities **Actions:**

- MInT consult with the Ethiopia Environmental Protection and other stakeholder MDAs to assess and consolidate any past national studies and efforts towards e-Waste management in Ethiopia.
- As deemed necessary from the assessments, develop an e-Waste management policy framework, law or regulations, and an implementation and communication plan for the same.

Outcomes:

- An environmentally friendly digital development

17 Administrative Reform and Change Management for Digital Government

Transforming public administration processes is an important aspect of digital public service delivery. Countries' experience shows that administrations that combine substantial reorganisation of how they work deliver better digital government services and get higher appreciation ratings from businesses and citizens. Business process reorganisation reduces cost, increases productivity, and provides flexibility in the delivery of online services. Reforms in business processes at MDAs, regional and local governments, and municipalities are essential to ensure that digital public services do not end up automating the already inefficient systems.

A government administrative reform strategy needs to support the digitalisation of the public sector in Ethiopia. While efforts were made to assess a government process when launching eServices, extensive business process transformations are not conducted in public institutions. The practice indicates that:

- Most of the business processes in the public sector were established decades ago and have continued unchanged. Despite some earlier business process reform (BPR) work by the government and changes in the expectations of customers, both internally and externally, the business processes, for the most part, have not been restructured. Many business processes that could be completed in one step or one location are fragmented between ministries/departments or sections within a given MDA or regional government. These processes must be reviewed and, if possible, re-engineered to achieve maximum Digital Government benefits.
- A vendor (Perago) performs the workflow analysis during the design of eServices, with some input from the service providers. The absence of business transformation means that, in most cases, no alterations are made to the existing manual process. Despite its role in service formulation across government, the Federal Civil Service Commission (FCSC) is involved in business transformation or workflow analysis before eServices are developed and launched.
- The Government uses management information systems (such as IFMIS, eProcurement, HRMIS, Tax MIS, Trade Facilitation System, Education MIS, Health MIS, Land management MIS, and Transport MIS). However, these are not based on reform and modernisation strategy; consequently, they are often inadequate and fragmented. The Government of Ethiopia needs to follow standard procedures such as ITIL and ISO 9000 certification to simplify, digitalise and optimise government services.

It is therefore important to:

- Ensure mandatory use of business process transformation and workflow analysis before launching digital public services.
- Assign the Digital Government Support Centre to develop and implement methodologies, standards, and tools for public administration reform and digital transformation. This includes the Services Transformation Toolkit for the administrative reform or modernisation before the design and rollout of their online services,
- Build the capacity at the Digital Government Support and other government branches on administrative reforms, workflow analysis, and standard procedures such as ISO 9000 to ensure that the GoE uses the latest tools and methodologies, criteria and principles for business process transformation and workflow analysis for eServices design and implementation.
- Invest in change management practices (training, skills, culture, knowledge, human resources incentives, etc.) on an ongoing basis to support digital transformation.

DGEN 18 – Administrative Reform and Change Management for Digital Government

Actions:

- Ensure mandatory use of business process transformation and workflow analysis before launching digital public services,
- Assign the Digital Government Support Centre with the development and implementation of methodologies, standards and tools for business processes,
- Build the capacity at the Digital Government Support and other government branches on administrative reforms and workflow analysis, standard procedures such as ISO 9000 and ITIL, and
- Invest in change management practices (training, skills, culture, knowledge, human resources incentives, etc.) towards digital transformation on an ongoing basis.

Outcomes:

- Modernization and transformation of government for improved service delivery,
- Increased citizens and business convenience, and
- Reduced costs of eServices development.

18 Cybersecurity and Business Continuity

Security and business continuity management are vital elements of digital public service because of growing cyber threats and the importance of public trust in digital services. Digital connectivity provides access to opportunities, jobs and efficient public services. At the same time, it exposes citizens and businesses to disinformation, online harassment, exploitation, abuse, theft and other harms. The COVID-19 pandemic has further shown the importance of cybersecurity, privacy, authenticity, integrity, and resilience of digital government transactions.

The GoE realises the importance of strong cybersecurity infrastructure to prevent unauthorised access to personal information. It established the Information Network Security Agency (INSA) in 2014 and set up a Computer Emergency Response Team - Ethio CERT. A regulation on cybercrime was also adopted in 2016. INSA published various documents on cybersecurity, including a draft National Cybersecurity and Strategy in 2021 and cybersecurity standard frameworks.[23] The Government has also established a Public Key Infrastructure (PKI) that ensures trust and security in digital government services, including digital identities and electronic signature.

However, key aspects of cybersecurity are still missing, including the National Critical Infrastructure Protection Plan and the alignment of cybercrime law with international best practices and standards. There is also limited progress concerning coordination with international organizations. Intra-MDA cooperation on cybersecurity issues is also important, especially among key institutions like INSA, MInT, Ministry of Peace, Ministries of Justice, and Defence. Most MDAs still need cybersecurity policies and protocols; those that do have developed them without input from MInT and INSA.

Some of the key issues facing cybersecurity include:

- Lack of up-to-date cybersecurity plan and strategy. There is a draft of the National Cybersecurity Strategy that needs approval, adoption, and implementation.
- No specific cybersecurity framework, regulations and procedures for identifying, designating and protecting national Critical Information Infrastructure.
- The public sector, especially the justice and law and order sector, has limited skills in cybersecurity and cybercrimes.
- The Public Key Infrastructure and Certificate authorities are not active.
- Scarcity of Cybersecurity professionals across MDAs and regional governments,
- Limited information, research, statistics and knowledge exchange on cybersecurity issues.
- Limited international collaboration on cybersecurity aspects,

[23] www.insa.gov.et

The ITU Cybersecurity Index measures cybersecurity in five dimensions, namely legal measures, technical measures, organisational measures, capacity building, and cooperation measures. It shows significant cybersecurity gaps in Ethiopia.

Box II – Five Measures of Cybersecurity

Legal and regulatory measures include the establishment of legislation identifying what constitutes illicit activities in cyberspace, together with the definition of the necessary procedural tools to investigate, prosecute and enforce such legislation, the establishment of cybersecurity baselines and compliance mechanisms, and procedures to ensure consistency with international obligations.

Technical measures cover mechanisms and institutional structures to deal with cyber risks and incidents, including setting up Computer Emergency Response Teams (CERTs) to respond to incidents using a centralized contact point and take quick and systematic action.

Organisational measures include ensuring that cybersecurity is sustained at the highest level of the executive, assigning relevant roles and responsibilities to various national entities, and making them accountable for the national cybersecurity posture. A national cybersecurity strategy (NCS) is often the key cornerstone of organizational measures at the national cybersecurity level.

Capacity-building measures cover all skills, resources, research and development training and awareness for reducing issues such as the digital divide and cyber risks. Capacity development tools and measures can contribute to managing cyber-related risks, protecting citizens, infrastructure, and businesses, and building stronger cyber communities.

Cybersecurity cooperation measures cover countries' bilateral and multilateral agreements, interagency, and public-private partnerships. Typical goals of cybersecurity cooperation include harmonization of minimum-security measures, information and good practice sharing, and codifying norms of behaviour.

Source: ITU, Global Cybersecurity Index

Ethiopia was ranked 115th out of 182 countries in the 2021 Global Cybersecurity Index—with a Global Cybersecurity Index score of 27.74, it was placed 21st among African countries. Ethiopia's score is three times lower than Mauritius, the regional leader.[24]

Source: International Telecommunication Union, Global Cybersecurity Index, 2021

[24] ITU, Global Cybersecurity Index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Development Level:
Developing Country, Least Developed Countries (LDC), Landlocked Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
27.74	11.56	4.46	8.03	3.69	0.00

Figure 24: Ethiopia's Score on Different Measures of Cybersecurity Index

The following action will be taken to advance cybersecurity within the context of digital Government and improve Ethiopia's standing in the Global Cybersecurity Index:

- Update and adopt a national cybersecurity strategy
- Develop a National Critical Information Infrastructure (CII) Protection Plan
- Expand National Coordination and Collaboration on Cybersecurity
- Improve Regional and International Cooperation
- Build cybersecurity skills
- Accelerate Research and Development and Knowledge Sharing on Cybersecurity
- Increase public awareness of cybersecurity.

18.1 Update and Adopt a National Cybersecurity Strategy

The draft national cybersecurity strategy developed by INSA in 2021 provides a starting point for developing a national cybersecurity strategy and policy. The document must be updated and widely discussed among all stakeholders for adoption. The government will draw on global practices and the latest experience in drafting and implementing cybersecurity strategies. It will amend the Computer Crime Act, considering global cyber threats.

DGEN 19 – Update and Adopt a National Cybersecurity Strategy

Actions:

- Review and update the cybersecurity strategy,
- Hold stakeholders' consultation,

- Adopt and implement a cybersecurity strategy.

Outcomes:

- Availability of a cybersecurity strategy that addresses cyber threats in a comprehensive manner,
- Implementation of cybersecurity strategy at all levels.

18.2 Develop a National Critical Information Infrastructure (CII) Protection Plan

The GoE will develop a National Critical Information Infrastructure Protection plan and policy that identifies, designates and protects all information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government. It will identify agencies and organisations with the responsibility and authority to implement the plan and take steps to enhance the security level of CII, as required. It will conduct regular risk assessments on the vulnerabilities of CII to prevent, protect, respond to, and recover from natural and malicious threats.

DGEN 20 – Develop a National Critical Information Infrastructure (CII) Protection Plan

Actions:

- Develop a National Critical Information Infrastructure Protection Plan and Policy,
- Consult CIIP plan, and
- Conduct regular risk assessments on the vulnerabilities of CII to prevent, protect, respond to, and recover from threats.

Outcomes:

- Availability of a National Information Infrastructure Protection Plan, and
- Improved protection of critical information infrastructure.

18.3 Expand National Coordination and Collaboration on Cybersecurity

Cyber Security is everyone's responsibility; therefore, MDAs and regional governments must make the necessary efforts to protect themselves, their citizens, and their businesses. Drawing on GEA security reference architecture, the government will adopt the security-by-design and zero-trust principle and coordinate with all MDAs and regional governments on all cybersecurity aspects to identify, protect, detect, respond to, and

recover from cyber threats. as per Reference Security Architecture. It will recruit more cybersecurity professionals to protect all public institutions' digital services. It will also ensure that core sectors like education, banking, transport and logistics establish CERTs that coordinate with the national CERT at INSA. It will ensure that the Ethio CERT team is consulted on every digital government project design and implementation to ensure the projects are aligned with at least minimum security requirements, security-by-design, and zero-trust principles.

DGEN 21 – Expand National Coordination and Collaboration on Cybersecurity

Actions:

- Improve cybersecurity coordination across, based on a Reference Cybersecurity Architecture,
- Recruit more cybersecurity professionals to protect digital public services, and
- Ensure that core sectors like education, banking, transport and logistics establish their CERTs.

Outcomes:

- Improved coordination on cybersecurity across the government,
- Increased identification, protection, detection, response, and recovery from cyber threats.

18.4 Improve Regional and International Cooperation

International and cross-border cooperation is important because cybersecurity is transnational. Participation in international discussions is key to learning progress and challenges in cybersecurity; thus, the GoE makes every effort to participate actively in developing and implementing international laws, agreements, treaties, policies, norms, and standards on cybersecurity. The government will coordinate and participate in international treaties and discussions, including those by the African Union, the United Nations and its agencies, international treaties like the Budapest Convention on Cybercrime and other global efforts to make cyberspace safe. It will ratify international agreements and enhance international cooperation (bilateral, multilateral) on cybersecurity.

DGEN 22 – Improve Regional and International Cooperation

Actions:

- Adopt regional and international cybersecurity agreements, treaties, policies, norms and standards, and

- Participate in international discussions and deliberation on cybersecurity.

Outcomes:

- Enhanced international cooperation, and
- Increased participation in international cybersecurity governance.

18.5 Build Cybersecurity Skills

Ethiopia's cybersecurity workforce is insignificant; thus, there is a need to increase the quality and quantity of specialists in this important area. The Government will expand the national cyber workforce, improving its diversity by mainstreaming cybersecurity and digital resilience subjects and degrees at both undergraduate and postgraduate levels. It will also include cybersecurity and cyber hygiene in the curriculum of all levels of education to equip students with relevant cyber knowledge and etiquette and self-protection from disinformation and online abuse. The government will also increase practical cybersecurity skills via hubs and accelerators and establish a cybersecurity professional certification/accreditation and career progression framework. There is also a need for providing specialised training for law enforcement experts and the judiciary. The Government will develop specialised cybersecurity training for civil services and the justice and law and order sector.

DGEN 23 – Improve Cybersecurity Skills

Actions:

- Mainstream cybersecurity and digital resilience subjects and degrees at both undergraduate and postgraduate levels,
- Include cybersecurity and cyber hygiene in the curriculum of all levels of education,
- Increase practical cybersecurity skills via hubs and accelerators, and
- Establish a cybersecurity professional certification/accreditation and career progression framework.
- Provide specific training for law enforcement and judiciary.

Outcomes:

- Availability of a critical mass of cybersecurity experts,
- Increased cybersecurity literacy in the law-and-order sector.

18.6 Accelerate Research and Development and Knowledge Sharing on Cybersecurity

While INSA provides information on cyberattacks on an ad hoc basis, there is limited data, research and knowledge on cybersecurity, cyber incidents and how to mitigate and recover. The academia, through a National Research and Education Network (EtherNet) and INSA, will launch research labs on different aspects of cybersecurity to facilitate knowledge sharing, covering aspects such as application testing, network access control, network behaviour monitoring, static and dynamic malware analysis, etc. Based on the different analyses, the researchers could guide government entities on scenarios of diverse cyber threats and how to prepare for business continuity and recovery. Ethio CERT will publish regular cybersecurity incidence statistics to provide evidence and input to research and innovation in this complex area. The research community will also increase investigation and publish analysis that can be used as a basis for decision-making in this growing area.

DGEN 24 – Accelerate Research and Development and Knowledge Sharing on Cybersecurity

Actions:

- Launch research labs on different aspects of cybersecurity,
- Expand research on cyber threats, and
- Publish evidence of cyber threats for facilitating decision-making.

Outcomes:

- Availability of cybersecurity research lab, and
- Increase the availability of evidence on cybersecurity to facilitate decision-making.

18.7 Improve Public Awareness of Cybersecurity and Cyberthreats

The more citizens and businesses access digital tools, the more they will be exposed to a wide range of cyber threats, from theft to disinformation, from online harassment to child abuse. The safety concerns to the public range from mental health and well-being challenges associated with being online for long periods to risks such as harassment and cyberbullying, access to harmful online content, misinformation,[25] mal-information[26] and

[25] Misinformation is when false information is shared, but no harm is intended

[26] Mal-information is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere

disinformation,[27] online gender-based violence or misuse of personal information by criminals for different gains. Thus, ongoing public awareness is critical. The Government will work with academia, media, civil society and other interest groups to empower end-users to keep themselves and their organizations safer online. Ongoing cyber hygiene and cyber safety training will be provided to ensure that everyone is protected.

INSA's cyber portal will be improved to provide more information on cyber threats, to gather and share knowledge on local and global developments in cybersecurity cyber defence methods and to provide guidelines for the public on how to protect oneself from cyberattacks and cyberstalking and reduce the risks. INSA will also create a platform for discussion among cyber experts who publicly exchange opinions on current threats and potential solutions.

DGEN 25 – Improve Public Awareness on Cybersecurity and Cyberthreats

Actions:

- Work with academia, media, civil society and other interest groups to empower end-users,
- Expand the INSA portal to provide more knowledge on cybersecurity.

Outcomes:

- Increased public awareness of cybersecurity issues.

[27] Disinformation is when false information is knowingly shared to cause harm

19 Accelerate Digital Inclusion and ePartication

Digital inclusion and e-Participation are important aspects of driving the use of digital government services. Baseline data in the introductory section of this Strategy shows that only about 4% of the Ethiopian population has some contact with digital government services; thus, there is work ahead to bring everyone online and ensure they use digital technologies to access government services. Most citizens and small businesses have limited or no Internet access and are excluded due to availability, affordability, and digital ability issues.

19.1 Accelerate Digital Inclusion

Digital inclusion is ensured via:

- Improved connectivity – when citizens and businesses are connected to affordable, reliable, and high-speed broadband infrastructure to access the Internet, applications and resources using affordable devices.
- Accessible user services - when digital government applications are designed to meet all users' needs in their preferred languages. Users include those with disabilities who are therefore dependent on assistive technologies.
- Digital skills – when citizens and businesses have adequate competence to use digital devices and the Internet for social and economic goals and can also protect themselves from the dangers of being online.

The GoE will ensure everyone, whether they are living with a disability, are culturally or linguistically diverse, have limited digital ability, or otherwise, can access and engage with digital government services. It will draft a digital inclusion policy that ensures systematic connectivity of citizens and businesses and improves digital skills, especially for marginalised groups such as people in rural and underserved areas, women and youth, older people, people with disabilities and internally displaced populations. The GoE will invest in connectivity infrastructure to improve Internet access (connection reliability and affordability) and apply human-centred design approaches in developing services to cater for all. Digital inclusion will emphasise omnichannel service delivery to ensure all services delivered digitally can be accessed over the phone or face-to-face so that no one is excluded.

The government will also ensure that:

- The design of digital government services considers access for citizens of all ages, abilities and economic backgrounds.
- Websites and services meet the latest Web Content Accessibility Guidelines,
- eServices are designed to take the cultural and linguistic diversity into account.

Awareness of the available digital government services is paramount for them to accept and use the e-services; thus, the government will create a services catalogue and disseminate it widely via different channels, including media.

DGEN 26 – Accelerate Digital Inclusion

Actions:

- Develop a digital inclusion strategy/policy,
- Improve broadband access to citizens and businesses,
- Increase inclusive digital government services, taking social, cultural, linguistic and economic consideration, and
- Improve digital skills for marginalized groups such as people in rural and underserved areas, women and youth, older people, people with disabilities and internally displaced populations.

Outcomes:

- Digital inclusion of marginalized groups, especially people in rural and underserved areas, women and youth, elderly, people with disabilities and internally displaced populations, and
- Empowerment of citizens and businesses.

19.2 Advance eParticipation

E-participation, involving citizens through digital consultation on future government legislation and regulation, current services and other concerns, is an important component of effective digital government. The GoE realises that stronger online public participation can improve the quality of political decisions and increase the perception of the decisions' legitimacy. A significant amount of social media use in Ethiopia indicates the potential for adoption of such a media for eParticipation.

The government will use digital technologies, such as social media, to improve interaction and connect citizens with the government to handle complaints and queries on digital government services. It will create a platform for "e-Ideas" for the public to contribute and suggest ideas for fostering innovation in the ICT field, including improvement in e-services. The digital government eParticipation platform will incorporate the following:

- A forum for electronic posting to encourage open dialogue, the expression of opinions and online discussions,
- A tool for electronic notes to gather views and build proposals from citizens,
- A system of email consultation to allow citizens to participate in the discussions across the whole of government, use of social networking sites (Facebook, X, etc.) to participate and interact with the public.

These platforms will be used to engage with citizens and businesses, handle citizen complaints, allow monitoring of complaints and inform citizens of government policies. Citizens and businesses can freely transmit their requests and share their concerns and ideas. The requests will then be directed to MDAs, regional government and local authorities as appropriate. A citizen can also keep track of their requests through a ticketing system. Data analysis from these platforms will be used to understand the population's needs and improve policies and resource allocation.

DGEN 27 – Advance eParticipation

Actions:

- Create online platforms for citizens' and businesses' engagement and
- Support open dialogue, the expression of opinions and online discussions

Outcomes:

- Improved leverage of online platforms for open dialogue, the expression of opinions and online discussions between government and citizens and
- Empowerment of citizens and businesses.

Part VI: Digital Government Essentials

20 Essentials of Digital Government

An extensive consultation with stakeholders reveals that Ethiopia's digital integration with the rest of Africa and worldwide and the financing of digital government services are indispensable. In the end, the digital government strategy considers these two essentials.

A significant movement of goods, services, and financial resources across the border is expected within the Africa Continental Free Trade Area (AfCFTA); thus, harmonising digital government solutions will foster trade, cross-border interaction, and cooperation. Digital transformation, such as single window customs services, has already reduced cross-border trade costs and connected more businesses and consumers globally. There are also partnership agreements between countries around the cross-border transfer of data and compatible e-invoicing and e-payment frameworks and common governance frameworks.

Financing of digital government is a necessary condition for its success. Implementing the Digital Government Strategy depends on our ability to mobilise technical and financial resources and implement priority programmes and projects based on prudent expenditure plans.

20.1 Integration of the Regional Dimension in Digital Government

The digital transformation of government is increasingly becoming a key aspect of the success of regional cooperation within the context of the Africa Continental Free Trade Area (AfCFTA). Regional integration thrives on borderless, user-friendly, end-to-end digital public services that facilitate the movement of people, goods and payments across countries. People should be able to move freely – either for work or privately – and access public services (e.g., health services) outside their home country.

Modern digital government services should not simply look inward but need to facilitate the free movement of goods, people and financial resources across borders. Digital government services should allow for harmonised electronic transactions, electronic invoicing, electronic payments, personal information protection, cross-border transfer of information, online safety and cybersecurity, digital identity, digital inclusion arrangements and dispute resolutions. The core principles of digital government, namely, digital by default, open by default, inclusiveness and accessibility, interoperability by default and mobile-first approaches, will encourage interaction across borders.

Regional digital cooperation also requires enhanced regulatory and legislative harmonization. Adopting the principles contained in European directives in data protection, electronic identity and trust, cyber security has already shown these can foster regional cooperation. The EU has issued the following directives that had a wider impact on regionalization.

- General Data Protection Regulation (European Parliament and Council, 2016),
- eIDAS Regulation - Electronic Identification, Authentication and Trust Services (European Parliament and Council, 2014),
- Directive on open data and re-use of public sector information (European Parliament and Council, 2019),
- Directive concerning measures for a high common level of network and information systems security across the Union (European Parliament and Council, 2016), and
- Directives on Public Procurement (European Parliament and Council, 2014[18]) (European Parliament, 2014).

Thus, designing a digital government by taking some of the key components of GDPR, eIDAS, common information, and network security will ensure the incorporation of regional dimensions.

The GoE's adoption of the underlying regulatory and legislative frameworks, such as the African Union Data Policy Framework and the African Union Convention on Cybersecurity and Personal Data Protection and their integration into revised government policies, legislations and guidelines will facilitate regional digital market within the framework of the African Continental Free Trade Area (AfCFTA). A harmonised digital identity framework, for example, will ensure the authentication of people across borders; thus, the digital government's identity registry action will take the African Union Interoperability Framework for Digital ID[28] that defines common requirements, minimum standards, and governance mechanisms for Africa in alignment with the different national legal frameworks into the account. The ID Interoperability Framework provides a common standard to digitally represent proof of identity issued by trusted sources from the AU Member States to ensure data systems interoperability across the region. The following actions will be taken to bring a regional dimension to the digital government:

- Integrate regional policy and regulatory frameworks and emerging regulations and strategies within the context of AfCFTA into revised legislation. These include the adoption of the African Union Data Policy Framework, the Interoperability Framework for Digital ID, the Convention for Cybersecurity and Personal Data Protection,
- Participate in international dialogues related to digital government and digital cooperation,
- Seek bilateral and multilateral cooperation to facilitate the flow of goods, people and finances across borders for trusted data flows and end-to-end digital trade. Cross-border partnership agreements in domains like harmonised electronic transactions, electronic invoicing, electronic payments, personal information protection, cross-border transfer of information, cross-border online safety and

[28] African Union, Draft Interoperability Framework for Digital ID, Unpublished

cybersecurity, digital identity and dispute resolution issues will be negotiated with countries as required.

DGES 1 – Integration of Regional Dimension

Actions:

- Integrate regional policy and regulatory frameworks and emerging regulations and strategies within the context of AfCFTA into digital government,
- Participate in international dialogues related to digital government and digital cooperation, and
- Seek bilateral and multilateral cooperation to facilitate the flow of goods, people and finances across borders.

Outcomes:

- Increased regional cooperation and trade, and
- Improved flow of goods, people and finance across the border

20.2 Mobilisation of Resources for Digital Government

The digital government requires substantial financial investment in infrastructure (data centre, connectivity, hardware and applications), eServices, training and capacity building. The Digital Government Strategy and Implementation Plan envisage a funding requirement of US$40 million to implement the activities, exclusive equipment, applications and human resources.

Thus, sustainable and transparent funding that supports the implementation of this Digital Government Strategy is essential. The Government will ensure that the Strategy is funded using local financial resources and a mixture of investment models, including universal access funds, public and private financing and development aid. Ministries, Departments, Agencies and regional governments need to allocate funding to upgrade existing digital services and roll out citizens' journey-aligned eServices and businesses' journey-aligned eServices.

At the same time, the GoE realises that funding of digital government depends not only on the amount of money being spent but also on how it is allocated; thus, ongoing evidence-based prioritisation of digital education financing is critical. The Government will carry out the following actions to improve the financing of the Strategy.

20.2.1 Mobilisation of Resources

The Government will set up resource mobilisation for digital government. Drawing on this strategy, the Government will prepare a short communication document outlining priority areas that need to be addressed in short-term and medium-term projects to

mobilise funding. The Government will also organize a resource mobilisation conference on digital government in coordination with development partners and the private sector.

DGES 2 – Develop a Resource Mobilisation and Communication Plan for Digital Government

Actions:

- Develop promotional documents and proposals for financing digital government and
- Work collaboratively with development finance institutions and multilateral development banks to mobilise financing digital government on priority digital government projects.
- Explore PPPs and partnerships with global tech firms and international development Agencies on the top of government resources to increase budget flexibility.

Outcomes:

- Availability of funding for priority digital government programmes.

20.2.2 Adoption of Cost-saving Measures

The GoE will also adopt strategies that accelerate the cost of implementation of digital government. Practices such as digital public goods and digital public infrastructure are essential for the long-term savings of digital government programmes. In this context, the Government will:

- Strengthen its procurement system, aligning it with Government Enterprise Architecture and interoperability standards, and improving inter-agency collaboration to reduce the cost of digital government projects,
- Pool government procurement through a one-stop shop,
- Adopt the GovStack building block approach to facilitate the reuse of components and applications.

DGES 3 – Adopt Cost-saving Strategies

Actions:

- Strengthen the procurement system, align it with Government Enterprise Architecture and interoperability standards, and improve inter-agency collaboration to reduce the cost of digital government services.
- Pool government procurement through a one-stop shop
- Adopt the GovStack building block approach to facilitate the reuse of components.

Outcomes:

- Optimal use of financial and technical resources and cost savings

21 Monitoring and Evaluation of Digital Government

The experiences of eGovernment strategies of 2011 and 2016 show that having a Strategy is the first step, but implementing the Strategy is the government's most important task. The success of the Digital Government Strategy will be measured via the progress that MDAs regional and local administrations make in achieving the five themes – connected government, user-centred services, data-driven decision-making and value, secured and trusted government and open access. The Government will measure:

- The level of increase in collaboration between MDAs and regional government towards interoperable architecture and a whole-of-government approach,
- The extent of adherence to interoperability principles such as once-only, digital-first, open data by design, privacy-by-design, security-by-design, cloud-first, mobile-first, etc.
- The extent of usage of eServices and availability of public sector data and services that are digital by design,
- The level and availability of online services that are inclusive, accessible and responsive to the needs of citizens, businesses, visitors and government staff,
- Extent of integrity, security and transparency in service delivery, which promotes trust in the government,
- The degree to which data were used for evidence-based policy and decision-making,
- The extent to which data were used for economic value creation by the public and private security and
- The extent of digital literacy, competency, and professional development of the government staff.

Data such as Internet uptake, number of eServices, and usage by citizens and businesses will be measured against baseline figures presented in Table 3. The success measures will also align with international benchmarks so that progress that we make on the quality of life of citizens and ease of doing business are reflected at international levels. The United Nations eGovernment Development Index (EGDI) provides a useful list of areas of eGovernment maturity measurement indicators, especially for eServices (availability of institutional organization data, content provision, e-participation/inclusion and technology frameworks). The Digital Government Readiness Assessment and GovTech Maturity Index are other tools that can be used to gauge our progress. Using these tools will allow the Government to have a uniform measure of progress and improve our international standing.

Table 9: EGDI and GTMI Indicators Themes

Electronic Government Development Index themes	Digital Government Readiness Assessment / GovTech Maturity Index Themes
• Presence of main portals • eServices, eParticipation, open data, eProcurement and secondary portals • Governance and coordination • Presence of CIO • Coordination between national and subnational • Core ministries participation – justice, planning, finance, health, education, trade • Legal framework • Access to information • Data protection • Cybercrime, cybersecurity • E-transaction • Digital signature • Digital identity, • E-procurement • digital publishing of government expenditure • interoperability and data sharing • open government data • emerging technologies • Digital Government strategy content • SDG alignment • Local development • E-participation • Data governance • Digital by default, digital-first, digital by design, once only principle • Emerging technology • Monitoring and evaluation • Foresight tool and scenario planning • User satisfaction survey • Regulatory sandbox and experimentation • Digital inclusion and e-participation	**Leadership, coordination, governance,** Vision, SDG alignment, institution, CIO and Funding **Digital skills** Skilled staff, availability of training, career path, talent development **User-centred e-services and channels** User-centred design principles, participation and feedback, omnichannel, private sector participation **Infrastructure** Data centre, Enterprise architecture, interoperability, ESB, Government Network, emerging technology, reusable components, contact centre **Legislation and regulation** Data protection law, digital transaction, digital identification, consumer protection, cybercrime, open access and PPP law **Data, data strategies and governance** Data management strategy, base registers, SDI, data sharing protocols, big data use and open data **Cybersecurity, privacy and resilience** Cybersecurity strategy, cybersecurity unit, CII protection plan **Public administration reform and change management** Business process reforms, availability of referential data and registries, change management practices

• Measures for connectivity and vulnerable group • eServices and e-participation, skills and connectivity for women and marginalized groups • Use of social media • User satisfaction survey	**Supporting digital ecosystem** Start-up programme, emerging technology skills, civil society participation

The GoE will draw on EGDI and GTMI indicators and existing baseline data that was gathered before the development of this Strategy to track progress. The digital government's key actions, key performance indicators and relevant GTMI and EGDI themes are provided in Annex III.

The GoE will monitor progress in all action areas. It will partner with universities and research institutions to promote studies on different themes of digital government. Ongoing user satisfaction surveys on digital government services will support monitoring and evaluation. In addition, the government will integrate monitoring and evaluation in implementing all the actions outlined in this Strategy and Implementation Plan. This will allow periodic reviews to adjust different activities and the entire digital government strategy. A midterm review of the digital government strategy will also be carried out to evaluate progress and refine the actions.

22 Way Forward

The Digital Government Strategy Implementation Roadmap that accompanies this document proposes three steps implementation - (i) preparatory stage that focuses on the development of plans (infrastructure modernisation plan, Digital Government Service Centre plan, eServices prioritisation plan), (ii) an implementation phase that focuses on delivering results in all the 14 strategic areas and (iii) a consolidation phase where lessons learnt from the two phases are used to accelerate the transition from Digital Government to GovTech.

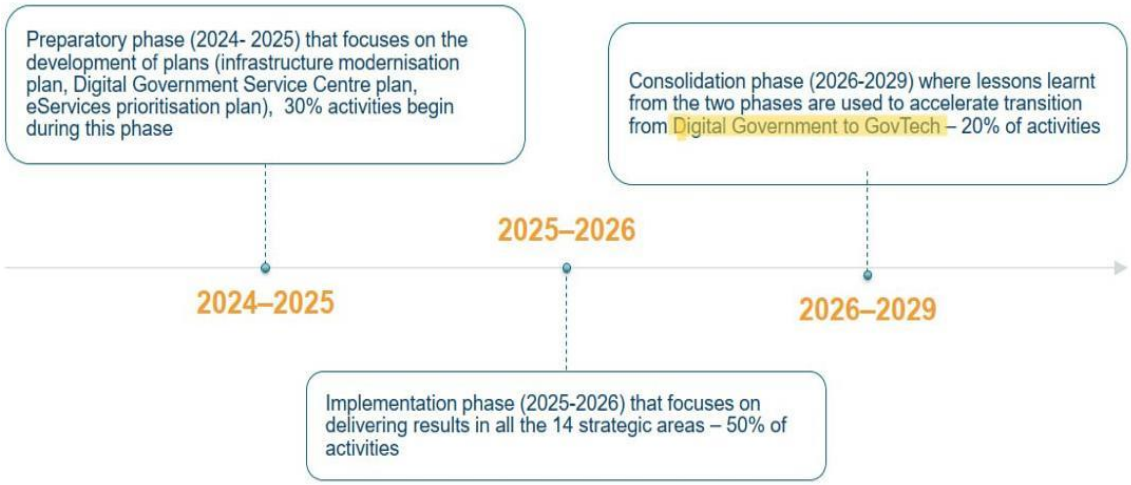

Figure 25. Implementation Roadmap

Delivering the sixty activities outlined in the Strategy requires considerable coordination; tackling them will require contribution and support from all government entities. Establishing a Digital Government Support Centre is central to the success of the Strategy. The implementation roadmap envisages an initial investment of US$40 million to deliver some of the core activities, exclusive of human resources and equipment. Resource mobilisation is thus another important task for ensuring success.

Annex I. List of Priority Back-office Applications Proposed by MDAs that Participated in the Survey

MDA	Proposed System
Ministry of Agriculture	• Registration & Competency Certification System • Livestock Identification and Traceability System • Agricultural commodities and inputs identification & registration system. • Agricultural Inspections system • Agricultural Certifications System • Agricultural Permits System • Veterinary Drug and Biological Device database, License and Permits System • Sanitary and Phytosanitary Management Information System • Animal and plant product Tracking/Tracing System
Ministry of Mining	• Mining Cadastre System • Minerals Export Certificate of Competence system
Civil Service Commission	• Civil Service Management Information System • Administrative Tribunal System • Recruitment, HR competency, Inspection and Performance Management System
Ministry of Transport and Logistics	• Freight Transport Operator Registration and Competency Certification System • Public Transport Operator Management System • Vehicle Importers and Assemblers Certification System • Construction Machine Registration, Permits and Competency Certification System • Driver and Vehicle Penalty Management System
Ministry of Trade and Regional Integration	• Online Trade Registration and Licensing System • Upgrading the e-Trade system
Ministry of Industry	• Manufacturing Industry Information System • Tamrit Coordination Mechanism and Information System
Ministry of Peace	• Conflict Situation Monitoring, Conflict Early Warning and Response System
Ministry of Justice	• e-Courts (Integrated Electronic Case Management) system
Ministry of Revenue	• Business Intelligence (BI) system • e-Invoice system • Risk Management and Appeal management system
	• Digital Monitoring and Reporting system

Ministry of Ministry of Planning and Development	• National Project Coordination and Lifecycle Tracking System • Climate Knowledge Management System • Population and Development Data Analytics System • Public Investment Management Information System
Ministry of Tourism	• Destinations Information Management System • Diagnostic assessment of the national and international payment systems • National Resource Information Management System (RIMS) • Digital marketing and Consumer feedback management systems
Ethiopian Communications Authority	• National Addressing System
Investment Commission	• Foreign Direct Investment Tracking system
Ministry of Labour and Skills	• Online Work Permit Application System • Labour Market Information System
Ministry of Foreign Affairs	• Investor Management System
Ministry of Culture and Sports	• Applications processing, travel support, accreditation, registration and renewal system • Approvals, Inspection and Rating System for cultural and art institutions and sports facilities • Integration of Document Authentication and Registration Information System
Document Authentication and Registration Services	• Integration of Document Authentication and Registration Information System
Public Servants Social Security Administration	• Social Security Administration system
Ethiopian Archives and Library Service	• Library, Archives and Record Management System

Annex II. Proposed Task Areas and Initial Membership of Technical Committees

Technical Committee	Strategy Task Area Coverage	Initial Member Organisation	Coordination
Coordination, Legal and Governance Technical Committee	• eGovernment Strategy Implementation Coordination • Prioritisation of Strategy Interventions • National Policy, legal and regulatory Issues • Government Enterprise Architecture Implementation issues • Technical Standards Development issues • Compliance and Conformance to Standards • Development and Compliance with E-Services standards, including UN eGovernment development Index indicators	**Ministry of Innovation and Technology** • Ministry of Planning and Development • Information Network Security Administration (INSA) • National Digital ID Program • Ministry of Trade and Regional Integration • Regions Representatives	Ministry of Innovation and Technology
Connected Government, GovStack, Registries and Applications Technical Committee	• Realising Government Systems Interoperability • Implementing the National Data Exchange Switch (Enterprise Service Bus –(ESB)) • Digitising the National Data Registries and Government Offices • Integrating building block and GovStack approach, • Connecting the National Data Registries to GSB, • Digitising the Government Offices • Software Development Back Office and G2G applications • Improving Payments Ecosystem	**Ministry of Innovation and Technology** • Immigration and Citizenship Service • National Digital ID Program • Ministry of Trade and Regional Integration • Ministry Of Mines • Ministry of Tourism • Ministry of Finance and Economy • Ministry of Planning and Development • Customs Commission • Civil Service Commission • Ministry Transport and Logistics • Land Registries • The Ethiopia Agricultural Authority • Regional representatives	Digital Government Support Centre
E-Services Development Technical Committee	• Services standardisation and prioritisation • Business process reform and workflow improvement	**Ministry of Innovation and Technology**	Digital Government Support Centre

	• Design of services based on journeys and user-centred principles • Service delivery channels	• All Ministries and Agencies who submitted their e-services needs • Regional representatives	
Infrastructure, Access and Security Technical Committee	• National Data Centre development • Cloud enablement • Government-Wide Area Network • Institutional networks • National broadband access development • Cybersecurity, Cybercrime and Data Protection • Mainstreaming the PKI and digital signatures into MDAs • Digital inclusion	**Information Network Security Administration** **Ministry of Innovation and Technology** • The Ethiopian Communication Authority • AA City Administration • Ministry of Justice • The Federal Police Commission • Immigration and Citizenship Service • National Digital ID Program • Ministry of Trade and Regional Integration • The Document Authentication and Registration Services • Immigration Nationality and Vital Events Agency, • Ministry of Agriculture • Regional representatives	Digital Government Support Centre
Digital Government Financing and Resource Mobilisation Technical Committee	• Digital Government Project Prioritisation • Digital Government Project Profile Development • Considering project proposals and terms of reference. • Public and private partnership potential assessment • Resources allocation (e.g., Universal Access fund)	**Ministry of Finance** • Ministry of Innovation and Technology • Ministry of Revenue • Ministry of Planning and Development • Ministry of Industry • Ethiopia Chamber of Commerce & Sectorial Association • AA Chamber of Commerce & Sectorial Association • Ethiopian National Bank • Ethiopia Development Bank • Ethiopian Investment Commission • Regional representatives	Digital Government Support Centre

Digital Skills and Emerging Technologies Technical Committee	• Digital literacy and skills for government staff • Digital skills for IT professionals • Emerging technology skills • Emerging technology innovation • Emerging technology forums	**Artificial Intelligence Institute** **Ministry of Innovation and Technology** • Science and Technology University • The Civil Service Commission • Information Network Security Administration • Ministry of Labour and Skills • Ministry of Higher Education • Ministry of Agriculture • Ministry of Industry • Regional representatives	Digital Government Support Centre

Annex III. Digital Government Performance Indicators and Links to EGDI and GMTI

Action Area	Outcome	Indicators of Success, KPI	Link to EGDI and GTMI Indicators
DIGITAL GOVERNMENT CORE – APPLICATIONS AND SERVICES			
APS 1: Establish a Digital Government Support Centre	Sustainable and integrated support to digital government applications and services Improved user-centred services, Improved digital government innovation	Operation of DGSC Appointment of Government CIO	Institution and CIO
APS 2: Support the Development of MDA and Regional Government Line of Business Back-office Systems	Availability of open MDA information system that share data and reuse components Improved delivery of eServices based on design back-office system development Improved digital government services	Number of lines of business applications and services Number of applications that share and reuse data Number of MDA and regional government applications that connect to ESB	interoperability and data sharing, Data sharing protocols
APS 3 Implement an e-Office System	Availability of comprehensive eOffice solution Progress towards a paperless government	Availability of a comprehensive e-office system Number of institutions that connect to digital government eOffice platform.	Shared service designed based on service transformation and business reform
APS 4 Develop and Upgrade Shared Enterprise Resource Planning (ERP) systems	Availability of cloud-based major government ERP solutions that conform to GEA and standards use GovStack building blocks (registry, identity, payment) and GSB, Improvement of sharing data across government to deliver better services	Number of shared ERP systems Number of users of shared ERP systems	Shared service designed based on service transformation and business reform
APS 5 Develop a Government Client Management System	Availability of cloud-based government client management system provisioned as Software as a Service that conforms to GEA and standards, uses GovStack	Availability of client management system Number of institutions that use	Government contact centre

	building blocks (registry, identity, payment) and GSB Improved service delivery to citizens, businesses and visitors	client management systems	
AP6 – Develop and Upgrade Common Platforms like Mobile, payment, SDI, eLearning Platform	Availability of upgraded and shared platforms - mobile service delivery, ePayment, SDI, eLearning, etc. Improved government service delivery Increased adoption of the building block approach	Number of institutions that connect to mobile service delivery, ePayment, SDI, eLearning, etc	Shared service designed based on service transformation and business reform
APS 7 - Develop and Deploy end-to-end eServices	Availability of user-centred eServices Availability of eServices catalogue Improved use of e-services	Number of user-centred e-Services % of the increase in user-centred eServices	eServices, user-centred design principles,
APS 8 - eServices Access Channel Transformation and Omnichannel Service Delivery	Improved users' convenience Increased use of e-services	Number of services available via multiple channels Number of services available through mobile applications % of the use of mobile applications	User satisfaction survey, omnichannel
APS 9 - Provide Incentive for Online Digital Government Service Delivery	Increased availability of digital public service Improved knowledge exchange and learning between MDAs, regional and local government on the delivery of excellent digital government services Recognition of good digital government service delivery that inspires the other agencies.	Number of awards and recognitions provided to best digital government services	eServices
APS 10 - Establish and Expand Core Registries for Digital Government	Increased use of digital identification for delivering public services Availability of integrated and shared core registries Adoption of standards for facilitating data exchange and sharing Increasing adoption of the EthioConnect ESB as a data integration and sharing platform	Number of core registries shared by institutions Published data standards Number of institutions that are connected to ESB to exchange data	base registers, SDI, data sharing protocols ESB
APS 11 - Establish EthioConnect Enterprise Service Bus	Availability of EthioConnect ESB, Integration of core registries and selected MDA services into the ESB and Accelerated digital public service through shared data	Operation of Enterprise Service Bus Number of institutions that are connected to ESB to exchange data	ESB
APS 12 - Diversify and Accelerate Digital	Availability of diverse digital payment systems that	Number of payment channels for	e-Payment

Payment System for eServices	increase convenience and quality of government services, Improved revenue collection Improved financial inclusion and empowerment.	end-to-end services % of the increase in online payments	
APS 13 - Consolidate eServices Delivery Portals	Availability of central government portals that provide one-stop end-of-end service, Improved user convenience, Optimal use of technical and human resources, and Enhanced delivery of government services	Number of main service portals % of the increase in the use of eServices portals	Presence of main portals
APS 14 - Accelerate Users' adoption of eServices	Improved use of eServices Increased convivence and access, Improved government services, revenue and empowerment of citizens.	Number of eServices users Number of completed end-to-end transactions % of the increase in eService usage	User satisfaction survey User participation and feedback
DIGITAL GOVERNMENT FOUNDATIONS			
DGF 1 - Rationalise and consolidate Government Data Centres	Government cost saving Interconnection, collocation and resource sharing, Improved energy savings Acceleration of a whole of government approach	Number of Government Data Centres Number of institutions that are connected to the data centre,	Data centre infrastructure
DGF 2 – Accelerate Cloud Transition	improved public sector resilience, business continuity Improved capability to keep up with technological development improved cost saving	Number of eServices available via hybrid cloud Number of government entities that are connected to the cloud.	Cloud First, cloud adoption
DGF 3 - Modernize WoredaNet to Establish IP Core Government Network	Improved access to secured and high bandwidth government services, Improved capability to keep up with technological development, Improved cost savings, Enhanced government services	Existence of core IP government networks Number of redundant links Number of institutions that provide a minimum of 1 Mbps/user	Government-Wide Area Network
DGF 4 - Modernise Institutional Local Area Networks	Increased access to reliable and secure government services Improved capability to keep up with technological development, Improved cost savings,	Number of reliable government networks	Government-Wide Area Network

	Enhanced government services,		
DGF 5 - Accelerate Universal Access to Broadband Connectivity	Increased access to reliable and secure government services, Digital inclusion and empowerment of citizens, Improved delivery of digital government services	Number of Internet users Number of internet users that also use government services	Digital inclusion Measures for connecting vulnerable group
DGF 6- Implement Enterprise Architecture and Interoperability Framework for Connected Government	Improved interoperability of government, Accelerated whole-of-government approach and Improved delivery of digital government services.	Number of shared government services	Enterprise Architecture and Interoperability Adoption
DGF 7 - Establish National Data Sets	Increased availability of data, including core registries Increased use of data for decision-making, research and advocacy Increased innovation and use of open data for economic development	Number of shared datasets % of government entities that are connected to ESB and share data sets	Data governance, shared data
DGF 8 - Establish a Data Governance and Sharing Framework	Formal framework for collection, management and sharing in place Enhanced data quality and sharing Increase in evidence-based policymaking, Increase innovation and use of open data for economic development	Governance framework Number of shared registries and sub-registries % of government entities that are connected to ESB and share registries	data sharing protocols, data governance base registers, SDI, data sharing protocols, data governance
DGF 9- Make Data Open via an Open Platform	Increased availability of open data Increased use of data for decision-making, research and advocacy Increase innovation and use of open data for economic development	Open data platform % increase of users of open data platforms on an annual basis	Open government data
DGF 10- Increase Data Analytics and Use	Enhanced data analytics and use Increase in evidence-based policymaking Increase innovation and use of open data for economic development	Number of training workshops on data use Number of private sector entities using open data Economic value of open data	Open government data
DGF 11 - Develop National Strategies for Emerging Technologies	Availability of well-developed strategies that guide emerging technology use in the economy in general, in the public sector in particular Full integration of emerging technologies in the economy	Publication of AI strategy Publication of Blockchain policy/strategy	Emerging technologies

	and public service delivery	Publication of Guidelines on big data IoT Strategy Publication of Cloud computing strategy	
DGF- 12 Create Platforms for Engagement on Emerging Technologies	Availability of forums for emerging technology innovators Acceleration of innovation in core emerging technologies Improved availability of emerging technology products and services	Number of participants in AI forums and working groups Number of participants in blockchain forums Number of participants in IoT development platforms Number of participants in data analytics forums	Emerging technologies
DGF-13 Develop Emerging Technology Skills and Research	Increase awareness of emerging technologies, Availability of critical mass of experts in emerging technology Improved research and development and innovation in emerging technologies	Number of experts with advanced AI skills Number of experts with advanced IoT skills Number of experts with advanced blockchain skills Number of experts with advanced Cloud computing skills	Emerging technologies
DGF 14 - Promote Regulatory Sandboxes and Financial Incentives for Innovative Emerging Technologies Solutions	Availability of regulatory sandboxes that encourage innovation, Availability of financial incentives for emerging technology startups and innovators Increase in critical mass of emerging technology experts and innovators Availability of innovative digital government solutions that leverage emerging technologies	Number of regulatory sandboxes Number of startups benefiting from sandboxes Amount of funding available for innovation in emerging technologies % of successful regulatory sandboxes that led to the commercialization of products	Emerging technologies
DGF 15 - Advance the Private Sector and Startup Ecosystem	Increased private sector participation in the delivery of advanced digital government solutions Increased private sector participation in the delivery of advanced digital government solutions Improvement in the startup ecosystem and gradual	Number of hubs Number of accelerators	Startup programs

	graduation of innovators into enterprises		
DGF 16 – Promote the Academic and Research Sector for Digital Government	Improved innovation, research and digital products and services that are incubated in universities Increase in critical mass of digital solutions and emerging technology experts and innovators	, Number of emerging technology skill graduates Number of digital incubation centres	Emerging technology Startup programs
DIGITAL GOVERNMENT ENABLERS			
DGEN 1 - Promote High-level Leadership and Sponsorship of Digital Government	Availability of a formal Digital Transformation Council that is mandated to promote digital government strategy and Increased coordination of the implementation of digital government.	Tangible leadership support of digital government % increase in resources allocated for digital government	Leadership Vision
DGEN 2 – Increase the Leadership Role of the Digital Transformation Council in Digital Government	Increased awareness of digital government, Increased coordination of the implementation of digital government	Digital Transformation Council plays a critical role in the implementation of the digital government strategy	Governance and coordination
DGEN 3 - Establish Sectoral Technical Committees on Digital Government	Availability of a Technical Committees to support decision-making and implementation of digital government. Enhanced implementation of digital government strategy based on practice, insight and data. Increase sharing of knowledge on digital government topics..	Operational Technical Committees on Digital Governance Number of meetings of the Technical Committees Number of reports of each of the Technical Committee to the government	Governance and coordination
DGEN 4 - Advance the Coordination Role of the Ministry of Innovation and Technology	Improved capacity of MInT to oversee digital government projects, including producing annual calendars and reporting to different bodies, Enhanced capacity of MInT to develop policies, guidelines and standards on digital government and Enhanced MInT capacity to coordinate with MDAs, regional government and all other players to create a community of digital government within the framework of a whole-of-government approach	Number of capacity-building workshops Number of experts trained in different aspects of digital government,	Governance and coordination
DGEN 5- Create a Platform for Cross-Government Coordination	Availability of face-to-face and virtual platforms for coordination on digital government between MDAs,	Number of face-to-face meetings between MDA on digital government	Governance and coordination

	regional and local governments, Improved coordination of digital government, Enhanced capacities of CIOs, CTOs, SOs and CDOs, Increased standardization and data sharing.	issues, Number of participants in face-to-face meetings, % of the increase in MDA participation in a virtual forum	
DGEN 6 –	Availability and operation of Technical Working Groups on different projects of digital government Improved technical discussion on digital government Enhanced implementation of the digital government strategy,	Number of technical working groups Number of reports of technical working groups	Governance and coordination
DGEN 7 - Develop Civil Servants' Digital Competencies – Literacy, Skills and Digital-driven Service Culture	Improved government staff's competencies, literacy, skills and digital-driven service culture for effective public service delivery, Enhanced retention of skilled government staff	Number of workshops for government staff Number of government staff that received competency training % of government staff with digital literacy	Skilled government staff, career path
DGEN 8 - Provide Digital Literacy Training for Decision-makers	Increased awareness of decision-makers on data and digital government issues Enhanced support for digital government	Number of digital literacy workshops for decision-makers Number of decision-makers that received competency-based literacy	Skilled government staff
DGEN 9 - Build Digital Skills for those Working on Digital Government Projects or Information Technology Departments at MDAs, Regional and Local Governments	Accelerated skills for IT professional staff at MDAs, regional and local government that enhance digital public service planning and implementation, Improved retention of skilled government professional staff	Number of workshops for IT professionals by digital government domains and types Number of IT professionals that received digital skills training	Skilled staff, career path
DGEN 10 - Increase the Supply of Digital Skilled Workforce	Increased supply of digitally skilled graduates Improved research and development on digital government topics	Number of STEM graduates in high schools Number of graduates in computer science Number of graduates in information technology	Skilled graduates
DGEN 11 - Increase Public Digital Government	Improved collaboration between government, CSO and	Number of awareness workshops	Digital inclusion

and Data Literacy	media on raising public awareness of digital technologies and digital government Enhanced awareness about digital services by citizens and businesses.	for the public by type of channel Number of media campaign hours	
DGEN 12 – Develop the Necessary Guidelines and Tools for the Operationalisation of the Data Protection Law within the Public Sector	Availability of data protection implementation instruments and Increased trust in government services through enhanced data protection	Publication of pertinent guidelines and tools for operationalising the Personal Data Protection Law in the public Sector	Data protection law
DGEN 13 - Amend and Combine Current Trust and Digital ID Laws	Increased trust in government services through enhanced electronic trust, identification and digital signature laws	Publication of eID, trust and signature law % of the increase in online transactions	eID law electronic signature law electronic transaction law
DGEN 14 - Revise Cyberlaw Considering Recent Global Developments in Cyber Threats	Increased trust in government services through new cyber laws Increased capacity to prosecute cyber threats	Publication of cyber law % of the increase in prosecution of cyber offences to cyber law	Cyber law
DGEN 15 - Adopt a Law Providing for Open Data	Increase access to open government data Improved innovation and decision-making.	Publications of open access law % of increase in open data due to the open access law	Open access law
DGEN 16 - Adopt Instruments for Promoting Digital Government, Interoperability and Enterprise Architecture Principles	Increased trust in government services through enhanced principles such as digital-by-default, once only, open-by-default, privacy -by-design, security-by-design, mobile-first, cloud-first Enhanced availability of shared services	Publication of guidelines or directives related to digital-by-default, once only, open-by-default, privacy -by-design, security-by-design, mobile-first, cloud-first % of the population that uses eServices	digital-by-default, once only, open-by-default, privacy-by-design, security-by-design, mobile-first, cloud-first
DGEN 17 - Develop Legislation on Emerging Technologies in Society and Government (Blockchain, AI, Data Analytics, IOT, Cloud Computing)	Availability of emerging technology laws, guidelines and regulations Accelerated use of emerging technologies for digital public services	Published laws on emerging technologies – AI, biochanin, data analytics, IoT Number of consultations on legislation on emerging technologies	Emerging technologies
DGEN 28 – Development and Adoption of Policies and Strategies for the Management and Control of electronic waste	An environmentally friendly digital development	Published policies , laws and regulation on e-Waste	Electronic waste management

		Number of publicity campaigns on e-Waste	
DGEN 18 - Administrative Reform and Change Management for Digital Government	Modernization and transformation of government for improved service delivery, Increased citizens and business convenience, Reduced costs of eServices development.	Number of rationalized e-services Number of eServices designed following workflow and process reform	Business process reform
DGEN 19 - Update and Adopt a National Cybersecurity Strategy	Availability of a cybersecurity strategy that addresses cyber threats in a comprehensive manner Implementation of cybersecurity strategy at all levels.	Published Cybersecurity Strategy	Cybersecurity and business continuity strategy
DGEN 20 - Develop a National Critical Information Infrastructure (CII) Protection Plan	Availability of a National Information Infrastructure Protection Plan, Improved protection of critical information infrastructure	Published Critical information Infrastructure Protection Plan	Critical information infrastructure protection plan
DGEN 21 - Expand National Coordination and Collaboration on Cybersecurity	Improved coordination on cybersecurity across the government Increased *identification, protection, detection, response, and recovery from cyber threats*	Number of sectoral CERTs Number of cyber threat incidents detected and responded to annually, % of the increase in cyber incidents, % of decrease/increase in cyber response	Cybersecurity and business continuity
DGEN 22 - Improve Regional and International Cooperation	Enhanced international cooperation Increased participation in international cybersecurity governance	Number of international cooperation events in which the government patriciate	Cybersecurity and business continuity
DGEN 23 - Build Cybersecurity Skills	Availability of a critical mass of cybersecurity experts Increased cybersecurity literacy in the law-and-order sector	Number and percentage of academic institutions offering cybersecurity course Number of experts skilled in cybersecurity	Cybersecurity and business continuity
DGEN 24 -Accelerate Research and Development and Knowledge Sharing on Cybersecurity	Availability of cybersecurity research lab Increase the availability of evidence on cybersecurity that facilitates decision-making	Number of publications on cybersecurity % of the growth of citation of cybersecurity publications in local and international journals,	Cybersecurity and business continuity
DGEN 25- Increase Public Awareness on Cybersecurity	Increased public awareness of cybersecurity issues	Number of awareness workshops and events	Cybersecurity and business continuity

		% of Digital Government users that participate in the workshops Number of materials posted on the INSA website % increase in access to the INSA website	
DGEN 26 Accelerate Digital Inclusion	Digital inclusion of marginalized groups, especially people in rural and underserved areas, women and youth, older people, people with disabilities and internally displaced populations,	Number of Internet users % of Internet users that use digital government services, Publication of digital inclusion policy	Digital inclusion
DGEN 27 Advance eParticipation	Improved leverage of online platforms for open dialogue, the expression of opinions and online discussions between government and citizens, Empowerment of citizens and businesses,	Number of e-participation platforms created. Number of eParticipation issues addressed % of participation requests that have been resolved	e-participation
DIGITAL GOVERNMENT ESSENTIALS			
DGES 1 - Integration of Regional Dimension	Increased regional cooperation and trade, Improved flow of goods, people and finance across borders,	% of regional frameworks that have been adopted Number of bilateral agreements on cross-border movement of goods, people and financial resources.	Regional cooperation
DGES 2 - Develop a Resource Mobilisation and Communication Plan for Digital Government	Availability of funding for priority digital government programmes	Amount of resources mobilised for implementation of digital government strategy.	Financing
DGES 3 - Adopt Cost-saving Measures for Digital Government	Optimal use of financial and technical resources and cost savings	% of resources saved through optimal cost-cutting measures (estimate)	Financing