ZIMBABWE

An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Delivering a seamless Government experience

2024

ZIMBABWE

An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Delivering a seamless Government experience

2024

FOREWORD

His Excellency, Dr. E. D. Mnangagwa
President of Zimbabwe

A Vision for a Digitally Transformed Public Sector

The rapidly evolving digital landscape continues to reshape the way governments interact with citizens, deliver services and make decisions. This worldwide, technology-driven trajectory has been widely embraced by administrations as a catalyst for economic growth, improved service delivery and enhanced citizen engagement. To stimulate action towards the achievement of these outcomes, it is incumbent upon Governments to formulate and implement requisite ICT policies that promote value delivery through a coherent and effective alignment of technology with national strategic objectives. This will enable administrations to remain competitive and relevant in the face of both internal and global dynamics.

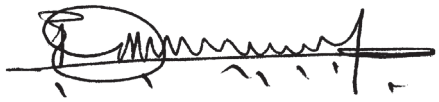
Desirous to modernise and transform public service delivery, the Government of Zimbabwe (GoZ) has developed a comprehensive Government Enterprise Architecture Model underpinned on the Whole-of-Government approach. Spearheaded by the e-Government Technology Unit, this strategic Framework is designed to guide the development, implementation, and management of information communication technology (ICT) systems and services across the entire public sector by providing a consistent approach to the acquisition, deployment and management of ICT infrastructure, applications, and processes. It sets forth the reference guidelines envisaged to enforce the alignment of government digital initiatives with the broader national developmental aspirations as enunciated through explicit goals and objectives outlined in successive national development strategies.

This milestone is testament to the commitment to leverage technology in the journey for the digital enablement of Government, ensuring that ICT investments are made strategically, and contribute to enhanced administrative efficiency, inter-agency collaborations, accountability, greater convenience and effectiveness driven by our profound desire to better serve the citizens. By establishing common standards, principles and guidelines, this Framework enables a coordinated approach to the implementation of the different activities and projects that will be undertaken to achieve these goals. It is anticipated that reference

to this framework will assist Ministries, Departments, Agencies, ICT professionals and other stakeholders involved in government ICT planning, implementation and management to smoothly navigate the digital government landscape.

The continued proliferation of ICTs and the subsequent hype to adopt ICTs across all socio-economic facets make it imperative for the Government to adopt a consistent and unified approach to guide digital transformation in the public sector. This Government Enterprise Architecture is a living document that will continuously undergo updates to reflect the changing needs and priorities of the Government. As such, stronger emphasis will be placed on adherence to the framework and Whole-of-Government approach in the implementation of all prioritised initiatives and projects. The principles and guidelines set forth in the Framework shall continue to empower the Government in its drive to harness the efficacy of technology to build a citizen-centric, accessible, inclusive and efficient government.

I therefore encourage all Government Ministries, Departments, Agencies, and stakeholders to embrace this framework and use it as an invaluable tool for guiding all ICT initiatives as we work together to achieve our shared vision of a digitally transformed Zimbabwe.



His Excellency, Dr. E. D. Mnangagwa
President of Zimbabwe

PREAMBLE

Dr. M. Rushwaya

Chief Secretary to the President and Cabinet

In recognition of the transformative potential of information and communication technology (ICT) in driving government efficiency, effectiveness, and service delivery, the Government of Zimbabwe set itself on a trajectory to modernize its administrative processes. This entailed harnessing the power of ICTs as a pedestal for driving the desired digital transformation. This decision resulted in several Ministries, Departments and Agencies embarking on autonomous digitalisation initiatives which demonstrated the immense appetite to replace manual processes with automated tools.

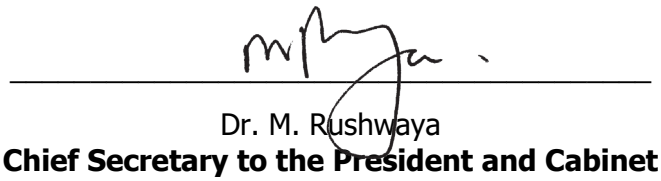
Despite the good intentions of independent computerisation efforts by MDAs, this culminated in a government digital ecosystem characterized by fragmentation, duplication, siloism, data inconsistencies, non-standardisation, incompatible systems and cost inefficiencies. The cost implications and inconveniences to the citizen became increasingly untenable and needed urgent redress. To navigate this complexity, the Government of Zimbabwe developed and introduced this Whole of Government Enterprise Architecture to guide the government's digital transformation journey.

The Enterprise Architecture provides a comprehensive roadmap for the development, implementation, and management of ICT systems and infrastructure across all government agencies in a holistic manner, ensuring that these are aligned with the government's overall strategic objectives. Principally, the EA framework therefore seeks to:

- Align ICT investments by the Government with strategic objectives and priorities.
- Enhance service delivery by streamlining operations to make administrative processes more efficient, accessible, and responsive services to citizens and businesses.
- Build a robust and sustainable digital government that is agile and capable of meeting the challenges and opportunities of the digital age.
- Promote interoperability and data sharing among government agencies.
- Enhance decision-making through data-driven insights.
- Promote transparency and accountability through digital technologies.

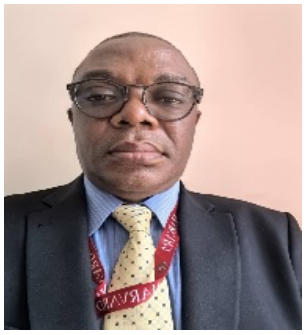
- **Drive economic growth:** Leverage ICT to stimulate economic development and create new opportunities for businesses and citizens.
- **Foster innovation:** Encourage innovation and digital entrepreneurship within the government and public sector.

This unified framework empowers government departments and agencies to streamline ICT initiatives, fostering a more agile and efficient public sector by providing a common language and approach to ICT planning, development, and implementation. The Whole-of-Government Enterprise Architecture emphasizes the alignment of ICT investments with strategic priorities to guarantee that technology serves the evolving needs of citizens, and drives sustainable development in line with the national vision.



Dr. M. Rushwaya
Chief Secretary to the President and Cabinet

PREFACE



Dr. T. Matekaire
Head, E-Government Technology Unit, Office of the President & Cabinet

This document outlines the government's vision for a digitally enabled public sector, where technology is used to enhance efficiency, transparency, and accountability. It provides a comprehensive roadmap for the development, implementation, and management of ICT systems and infrastructure across all government agencies. It advances the goal of the current Government digitalisation strategy, **Roadmap for an Integrated e-Government Ecosystem (2021 – 2025)** which seeks to establish a cohesive and seamless e-government ecosystem. It seeks to consolidate, coordinate and optimize government ICT infrastructure, and applications for the delivery of efficient and reliable government services.

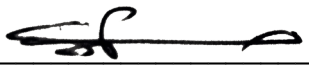
Realising that a structured framework is indispensable for successful e-government planning, implementation and management, it became obligatory for the Government of Zimbabwe to undertake Enterprise Architecture Modelling as a crucial step to consolidate the government ICT ecosystem and guide future ICT investment in public sector institutions. The Government of Zimbabwe developed this EA framework which contains reference architecture models, standards, principles, security and governance models covering all the architectural domains. The EA is meant to govern how Ministries, Departments and Agencies, processes and information systems should function together as a cohesive whole in the quest to deliver convenient citizen-centric services.

Since the inception of the project in 2022, the e-Government Technology Unit in the Office of the President and Cabinet adopted an inclusive and all-stakeholder approach to the development of the architecture model. The process was kick-started by a **High-Level Inception Briefing Workshop and Peer Learning Event** attended by senior government officials, development partners, civic organisations, professional bodies and ICT experts which set the tone for this groundbreaking undertaking. A series of workshops, discussions and interviews followed with relevant stakeholders to gather an in-depth understanding of the Zimbabwean context. Workshops and visits were conducted across all Ministries to assess their EA maturity. This was a fundamental stage in beginning the process of change management for government digitalisation.

This framework is the result of the extensive consultations and contributions from relevant stakeholders who committed to the development of the Enterprise Architecture for the Government of Zimbabwe. The entire process was rooted in the principle and desire to develop a home-grown architecture model that responds to the Zimbabwean demands. This Enterprise Architecture for the Government of Zimbabwe is therefore a result of the co-creation efforts with the e-Governance Academy (eGA), Estonia, who provided expert guidance to the entire process.

As a living document, the architectural artefacts will undergo periodic reviews and updates to align with government business strategies to ensure that the government continuously positions itself to better respond to the dictates of good e-government service delivery. This shall entail redefining of processes, information systems and infrastructure that support it, a process that requires the continued involvement of all stakeholders. The framework and all its associated documents become an important reference repository accessible to the entire public sector.

I extend my heartfelt congratulation to all stakeholders who dedicated themselves to the development of this framework; a game changer which marks the beginning of an exciting journey ahead that I believe everyone is enthused to be part of. It is a significant achievement that will ultimately lead to the strategic alignment of government digital enablement initiatives to national objectives as we strive to build a modern, responsive and agile Government that better serves its citizens.



Dr. Tafara Matekaire
Head, e-Government Technology Unit
OFFICE OF THE PRESIDENT AND CABINET

Introduction

The Government of Zimbabwe is honoured to present the Enterprise Architecture (EA) for the Government of Zimbabwe, a transformative blueprint designed to catalyse the nation's ambitious journey towards digital transformation. This EA has been meticulously developed by e-Governance Academy (eGA) experts in collaboration with the e-Government Technology Unit under the Office of the President and Cabinet, marking a critical step in Zimbabwe's march toward achieving its Vision 2030 of becoming an upper-middle-income economy.

Aligned with Zimbabwe's National Development Strategy (NDS) 1 and 2, the EA provides a comprehensive and unified digital framework that ensures the alignment of Ministries, Departments, and Agencies with the overarching national EA. This alignment is key in enabling the delivery of modern, citizen-centric e-services that empower individuals, businesses, and communities across the country. By integrating advanced digital technologies, the EA supports the Government's mandate to enhance service delivery, transparency, and efficiency within the public sector.

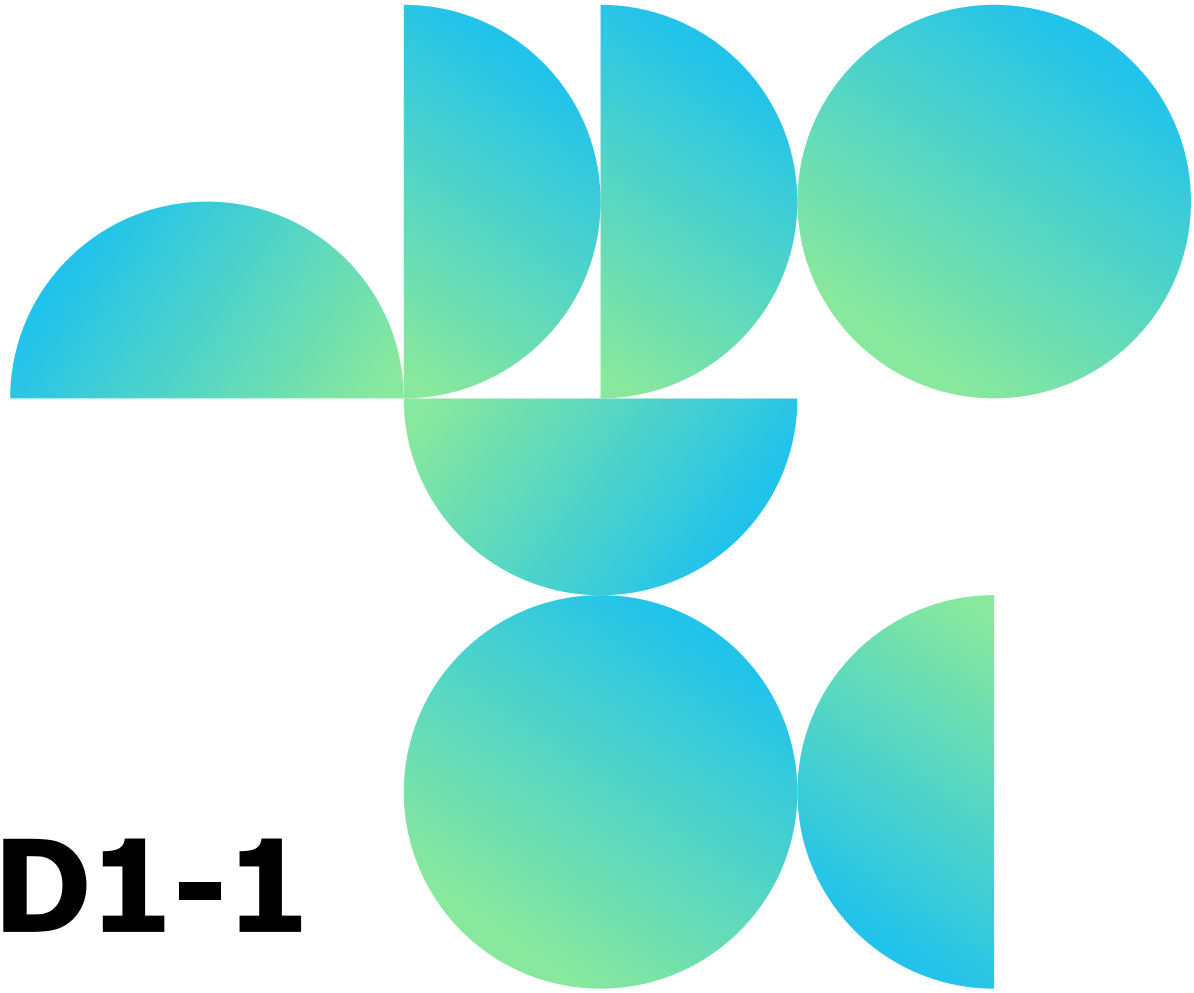
At its core, the EA serves as a strategic guide for Zimbabwe's digital economy transformation, facilitating the shift from traditional operations to a seamless, interconnected digital ecosystem. It is a critical tool for enabling Zimbabwe's MDAs to drive e-Government initiatives, ensuring that citizens benefit from convenient, accessible, and secure digital services that contribute to economic growth, social inclusion, and national development.

In line with global trends, Zimbabwe is positioning itself at the forefront of utilizing Information and Communication Technologies to anchor national development, strengthen its economy, and improve governance. The EA will act as a catalyst for building a knowledge-based economy and an innovative society, creating opportunities for all Zimbabweans to thrive in a rapidly digitizing world.

This comprehensive architecture outlines a clear strategy, supported by trained personnel, effective change management, and a phased roadmap for implementation. Once fully realized, the digital transformation driven by this EA will enhance the well-being of Zimbabwe's citizens, stimulate sustainable economic growth, and ensure the nation's long-term global competitiveness.

eGA extends its sincere gratitude to the Government of Zimbabwe for its unwavering commitment, collaborative spirit, and visionary leadership. This enterprise architecture not only paves the way for the country's digital future but also ensures that the dividends from this transformation are felt across all sectors of society, propelling Zimbabwe into a prosperous, digitally enabled future.

Index



D1-1 Situation Analysis Report

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Index of Figures

Index of Tables

Glossary

Abbreviations

Abbreviation	Definition
ACMM	Architecture Capability Maturity Model
BTEP	Business Transformation Enablement Program
CIO	Chief Information Officer
CERT	Computer Emergency Response (or Readiness) Team
CIRT	Computer Incident Response Team
COBIT	Control Objectives for Information Technologies
CTO	Chief Technology Officer
DC	Data Centre
EA	Enterprise Architecture
eGA	e-Governance Academy, Estonia
GDP	Gross domestic product
GISP	Government Internet Service Provider, Zimbabwe
GoZ	Government of Zimbabwe
ICTs	Information and Communication Technologies
ID	Identity
ITU	International Telecommunications Union
MDAs	Ministries, Departments and Agencies, Zimbabwe
MICTPCS	Ministry of ICT, Postal and Courier Services, Zimbabwe
MSMEs	Micro, Small, and Medium Enterprises
NDC	National Data Centre

Abbreviation	Definition
NDS1	National Development Strategy 1
OPC	Office of the President and Cabinet, Zimbabwe
POTRAZ	Postal and Telecommunications Regulatory Authority, Zimbabwe
RIDA	Rural Infrastructure Development Agency
SLA	Service-Level Agreement
TOGAF	The Open Group Architecture Framework
WoG	Whole-of-Government
ZGEA	Zimbabwe Government Enterprise Architecture
ZINARA	Zimbabwe National Road Administration
ZRP	Zimbabwe Republic Police

Terms

Term	Definition
Application	software that is dependent on the services of an operating system
cybersecurity	(a) the security of cyber devices and (b) security against threats created through the operation of cyber devices. Security usually means a situation where risks are not materialised
Data	reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing
Data exchange	data exchange, storing, accessing, transferring, and archiving of data
Digital signature	signature based upon cryptographic methods of the originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified
Digital governance	electronic governance, the application of information and communication technology (ICT) for delivering government services, exchange of information, communication transactions, integration of various stand-

Term	Definition
	alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back-office processes and interactions within the entire government framework
Digital government	using the tools and systems made possible by information and communication technologies (ICTs) to provide better public services to citizens and businesses
E-identity	a collection of data that connects the person with his/her physical identity in an electronic environment
e-services	library services delivered via electronic means, whether from local servers or provided via networks
(Government) Enterprise Architecture	a whole-of-government approach to support government ecosystems by transcending boundaries to deliver services in a coordinated, efficient, and equitable manner
interoperability	the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, using the exchange of data between their ICT systems.
Open data	data that can be freely used, re-used and redistributed by anyone without restrictions from copyright, patents or other mechanisms of control
Whole-of-Government	joint activities performed by diverse ministries, public administrations and public agencies to provide a common solution to particular problems or issues

1 Executive Summary

This report presents a comprehensive situation analysis of Zimbabwe's digital landscape to provide the Government of Zimbabwe with critical insights to expedite digital transformation and facilitate the development of a Government Enterprise Architecture. It analyses the essential pillars of digital readiness that are critical for fostering sustainable digital development and for strategizing future actions to enhance digital governance.

The findings and recommendations of this report are the result of extensive desk research, a review of public documentation, and the synthesis of data gathered from two online surveys, followed by conducting on-site interviews in Zimbabwe in January 2024 with key stakeholders.

The report was developed by the digital government experts of the e-Governance Academy – Dr Rozha Ahmed, Marit Lani, Tõnis Mäe, Toomas Mölder, Piret Saartee, Heiko Vainsalu, and Dr Uuno Vallner, with the kind support of Moffat Nyamadzawo.

The authors extend their gratitude to the dedicated participants from the Office of the President and Cabinet (OPC), the Ministry of ICT, Postal and Courier Services (MICTPCS), as well as representatives from all other Ministries, Departments, and Agencies (MDAs). Their active involvement through surveys and contributions during interviews was instrumental in enriching this analysis with significant insights and perspectives.

2 Introduction

2.1 Objectives

This situation analysis aims to evaluate the current state of the digital readiness of the public sector of Zimbabwe, and draw general findings in nine essential pillars of digital governance:

1. Political support, strategy
2. Coordination
3. Cybersecurity
4. Data management, secure data exchange
5. E-identity, digital signatures
6. Access to services
7. Digital skills
8. Digital engagement
9. Cooperation

Additionally, the analysis extended its focus on **Enterprise Architecture (EA)**. Based on two completed online surveys and on-site interviews with key stakeholders, findings are drawn that will facilitate the Government Enterprise Architecture modelling for Zimbabwe. The EA situation analysis looks at the progress made towards establishing an EA in Zimbabwe, examines the related key enablers and presents the results of online surveys carried out among the Zimbabwean MDAs.

The insights gained will provide the MDAs with a good understanding of the current digital landscape and the results can be used as a foundation and inspiration to underpin the next actions and pave the way for modelling a robust Government Enterprise Architecture that is responsive to the needs of the country.

2.2 Methodology

The situation analysis was conducted in five steps:

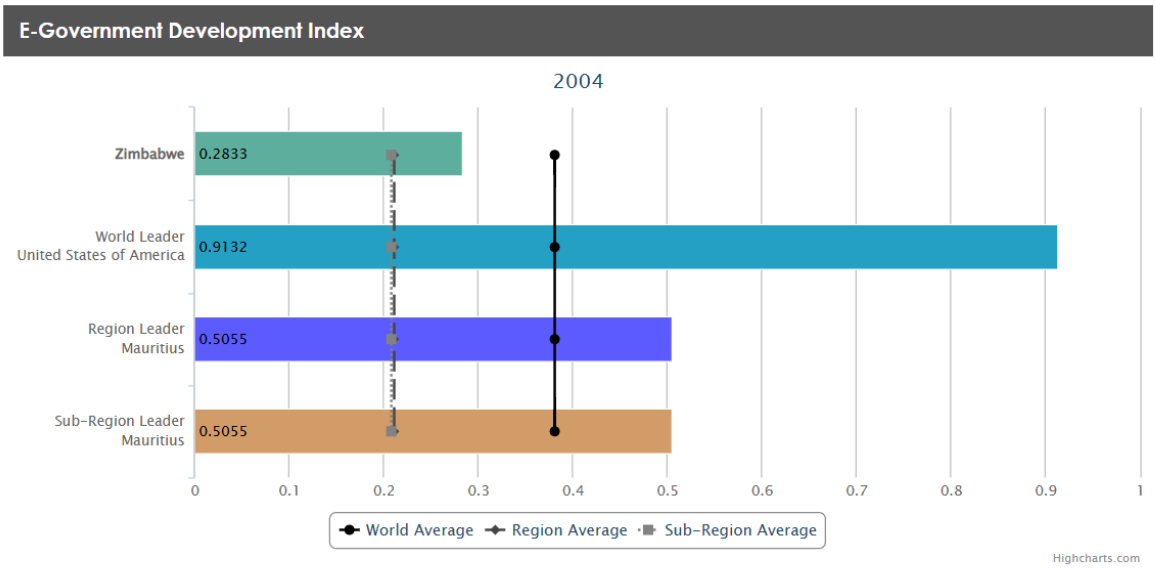
1. **Desk research**: review of existing policy documents, strategies, government political agenda, public reports, statistical sources, etc.
2. **Online surveys**: firstly, two public authorities in charge of digital issues – the Office of the President and Cabinet (OPC) and the Ministry of ICT, Postal and Courier Services (MICTPCS) in Zimbabwe – filled out a questionnaire that mapped the existing digital governance situation and stakeholders in Zimbabwe (hereafter: digital governance survey). Secondly, a more technical survey focused on EA (hereafter: EA survey) was created and disseminated to 48 MDAs

and 46 answers were collected using the LimeSurvey online survey tool, with 43 full responses.

3. **Interviews with key stakeholders** were conducted in Zimbabwe in January 2024 to fully understand the strategic goals, operational processes, obstacles, and technology requirements of the MDAs.
4. **Development of the situation analysis report**: the report was compiled, based on the input from desk research, online surveys, and on-site interviews.

2.3 Country Context

Zimbabwe is a southern African country lying north of the Tropic of Capricorn. South Africa borders it to the south, Botswana to the southwest and west, Zambia to the northwest, and Mozambique to the northeast and east, with an area of 390,757 square kilometres and a population of approximately 15,418,674 (2023 est.).[i] Zimbabwe is a low-income country with a GDP per capita estimated at 1,267 USD in 2022.[ii] The sanctions imposed on the country over two decades ago, COVID-19 and the effect of climate change have significantly impacted the Sub-Saharan country's economic potential. However, a raft of economic policies, vast natural resources and agriculture have been influential to counter the negative impacts of sanctions and the adverse environmental challenges.



E-Government Development Index	2024	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Zimbabwe (Rank)	149	138	126	146	134	126	133	129	137	120	130	116
Zimbabwe (Value)	0.44807	0.47170	0.50190	0.36920	0.34722	0.35845	0.35831	0.32304	0.30000	0.33161	0.28330	0.30438

Figure 1: Zimbabwe in the UN Digital Government Development Index 2024

https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/192-Zimbabwe/dataYear/2004

In 2024, 49% of the population had access to electricity. Internet use by individuals was reported at 35% in 2021,[iii] with 1.27 fixed broadband subscriptions[iv] and 88 mobile cellular subscriptions[v] per 100 people in 2022.

In the United Nations e-Government Development Index of 2024, Zimbabwe ranked 149th out of 193 countries. Other notable rankings include 141st (out of 193 countries) in the e-Participation Index 2024[vi] and 157th (out of 180 countries) in the Corruption Perception Index 2022.[vii] ITU ranked Zimbabwe 98th in their Global Cybersecurity Index 2020.

3 Situation Analysis on Public Sector Digitalization

3.1 Political Support and Strategy

Effective political leadership is essential for adopting digital governance, requiring high-level commitment from authorities such as the President or Parliament. This commitment involves budget allocation, mindset shifts among officials, a desire to re-engineer services, as well as monitoring enforcement through established authorities and ensuring digital integration across all policies and industries.

Based on the analysis of the collected information, there is strong support from the government level towards the implementation of digital government and a common understanding among the government institutions of the importance of digital transformation.

The government has dedicated the **E-Government Technology Unit in the Office of the President and Cabinet (OPC)** as the champion, coordinator and promoter of all government digital transformation initiatives.

Since 2012, the country has established several strategic documents that include various plans and visions for reform, as well as the establishment of official bodies and authorities to oversee the streamlining of digital transformation in the national development plans.

National Development Strategy 1 (NDS1, 2021-2025)[viii] was developed as the first 5-year medium-term plan to "improve access and usage of ICTs" and achieve improved service delivery through online digital platforms as some of its major outcomes under the Digital Economy Priority Area. The government has also prioritised ICT infrastructure, where it intends to have internet access at the village level by 2030 through the extension of the fibre optic backbone and last-mile connectivity. During the NDS1 period, the government targets increasing the internet penetration rate from 59.1% in 2020 to 75.4% by 2025. Further, the mobile penetration rate is also expected to be increased to 100% by 2025. Additionally, the government aims to develop a critical mass of appropriate ICT skills within the public sector and among citizens whilst prioritising the implementation of an effective change management program to ensure improved adaptation of ICTs.

The Transitional Stabilisation Program (TSP) 2018-2020[ix] was implemented and aimed at stabilising the macro-economy and the financial sector, introducing necessary policy and institutional reforms to transform the economy into a private sector-led economy, as well as launching quick wins to stimulate socio-economic growth.

Zimbabwe Vision 2030[x] was developed by the government to transform Zimbabwe into a "prosperous and empowered upper-middle-income economy by 2030". E-

government implementation is one of the objectives of the "Infrastructure Development Pillar", aiming to use information and communications technologies as a tool to enhance the efficiency of public services.

In addition to the aforementioned documents, based on the EA survey filled in by 46 respondents, several MDAs are either formulating or have already put in place sector-specific comprehensive strategies for digitalization and associated action plans. For instance,

- The MICTPCS launched a Strategic Plan and the Smart Zimbabwe Master Plan. The next effort is to develop SMART Zimbabwe 2030[xi] as an ICT master plan document to guide the sector's contribution to economic growth in line with the Government's Vision 2030. This masterplan will guide the specific innovations that Zimbabwe's industries will utilise in the digital future.
- The Ministry of Health and Child Care has adopted a National Digital Health Strategy for 2021-2025[xii] and an ICT Policy Framework.
- The National Prosecuting Authority has implemented an ICT strategic plan.
- The Postal and Telecommunications Regulatory Authority, Zimbabwe (POTRAZ) has rolled out a strategic plan 2019-2023[xiii] alongside a National Broadband Plan 2023-2030[xiv].
- The Rural Infrastructure Development Agency (RIDA) has established an ICT Policy, Disaster Recovery Plan, and an Annual ICT Maintenance Plan.
- The Zimbabwe National Road Administration (ZINARA) has put into effect an ICT Strategy for 2023-2025 and a plan for revenue system implementation.
- TelOne has embraced strategies for cloud computing, development of digital platforms, and modernization of their network, including fibre and LTE technologies, as well as introduced digital products and services.
- Finally, the Zimbabwe Republic Police (ZRP) has adopted a strategic plan, an ICT tactical plan, frameworks for smart policing and traffic management, as well as documentation for case management system requirements.

The EA survey was conducted by eGA in December 2023 and completed by representatives from various MDAs, encompassing 46 respondents, reveals that a substantial majority, 69.8%, rank digitalization as a top priority within their institutions, while the remaining 30.2% still consider it to be an important aspect despite it not being their primary focus.

According to OPC and MICTPCS officials who took part in the digital governance survey, the government's high **priorities** include digitalization of government operations, including other sectors like energy, education and health; information security; ICT infrastructure development and management, and management of road and transport administration. Medium priority was given to aspects such as the interoperability framework, the legal framework for digital governance, e-identity, and digital

engagement, while digital skills training for citizens was not pointed out as a particular focus area.

Regarding the **legal framework,** the existing relevant general laws in Zimbabwe have not been fully adjusted to align with the digital transformation agenda. However, the outstanding Electronic Transactions and Electronic Commerce Bill of 2013[xv] is one of the government initiatives to establish a legal framework for electronic transactions, electronic commerce, and digital signatures, which was approved in 2021.[xvi] Other relevant legislations and policies include the Access to Information and Protection of Privacy Act, 2003[xvii]; the Freedom of Information Act, 2020[xviii]; the Cyber and Data Protection Act, 2021 as well as the Zimbabwe National Policy for ICT.

The interviewees emphasized a critical challenge in the realm of digital transformation, citing the absence of a relevant regulatory framework as a primary obstacle. They expressed concerns that this lack of relevant legislation hampers progress in digital initiatives. Moreover, they pointed out that the process of updating and enacting new legislation is frustratingly slow, compounding the issue. This slow pace in legislative evolution, coupled with the absence of targeted regulations for digital transformation, is seen as a significant impediment, slowing down innovation and adaptation in an increasingly digital world.

3.2 Coordination

Digital governance requires a designated institution with decision-making authority across the administration. While regional solutions are viable, coordination is essential, not to centralize but to align decisions. This institution's strategic role in building digital governance is crucial, and its authority should be legislatively defined to give it directive power.

Concerning the organizational structure for the establishment of digital government in Zimbabwe, as stated in the previous section, the e-Government technology Unit situated within the OPC holds the responsibility for orchestrating **coordination** efforts, while MICTPCS is the technical implementing partner charged with the implementation of the national ICT policy and **development of digital government connectivity infrastructure, and software applications for** MDAs if such development is not sub-contracted. Furthermore, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)[xix] was established according to the Postal and Telecommunications Act Chapter 12:05 in 2001, to be the regulatory authority of Zimbabwe and also the data protection authority as enunciated in the Cyber and Data Protection Act, 2021 Data Protection Act, 2021.

Officials from the OPC and MICTPCS who took part in the digital governance survey pointed out several ongoing or forthcoming public sector **Digital Transformation Projects** identified towards digitalization. These include initiatives relevant to the

National Data Centre Upgrade and the disaster recovery site to be implemented between 2023-2025; e-Government Enterprise Architecture Modelling for 2023-2028; an Integrated Electronic Case Management System to be implemented in 2022-2025; a government e-mail system planned for 2024; Zimbabwe Electronic Single Window for 2023-2025; and the revamping of the Zimbabwe Government portal in 2024, which was adopted in 2018. Other ongoing projects highlighted include the Smart Education/e-Learning Project, the Smart Health Project, Community Information Centres, Government Network Consolidation, and National Broadband Connectivity.

The EA survey responses indicate that several Ministries and large public agencies have different designated roles to oversee ICT adoption in public institutions, 46.5% of participants noted several MDAs have established a role equivalent to the Chief Information Officer (CIO) position in charge of ICT adoption, or an ICT Manager. However, a network for CIO cooperation across the public sector is lacking, and there hasn't been a focus on organized training or ongoing skill development for CIOs. 41.9% of participants from MDAs have designated a role responsible for deciding on technologies and large-scale setup of solutions, which is usually also responsible for organization ICT architecture (the specific designation level - chief director, director or deputy director - was not exposed in the survey). Some 34.9% of participants confirmed that they have a Chief Development Officer role responsible for ensuring ICT-related changes. Of the respondents, 25.6% indicated they have a Chief Data Officer or Data Steward role responsible for data semantics, quality, and data management principles.

Interviewees and digital governance survey respondents from OPC and MICTPCS noted that full implementation of budget planning principles is developed and enforced by the law. Hence, the total yearly cost and resources are planned at the national level through the Public Finance Management System (PFMS), which is under the Ministry of Finance, Economic Development and Investment Promotion, and to some extent, budgeting is based on the long-term strategy. However, implementation of a designated separate budget for ICT and digitalization at the Ministry and Government agency level is still limited. In the EA survey, 48.8% of the participants considered the cost of digitalization to be the strongest obstacle in their institutions. External funding is used to support digital transformation in Zimbabwe, with the main international donor organizations being the World Bank (WB), African Development Bank, German Development Agency (Deutsche Gesellschaft für Internationale Zusammenarbeit, GIZ), Asian Development Bank (ADB), International Telecommunication Union (ITU), United Nations Development Program (UNDP), and United Nations Children's Fund (UNICEF). External funding is managed and coordinated through the Ministry of Finance, Economic Development and Investment Promotion.

3.3 Cybersecurity

The growing cyber threats in the world require public administrations to focus on digital governance security measures. It is important to be aware of the threats posed to digital governance. The coordinating institution is required to organize the development, monitoring and supervision of relevant cybersecurity rules and measures. A designated organization in the form of a CERT/CSIRT should be established, proper audit processes established, and all Ministries and authorities should be aware of and use adequate security measures. The cybersecurity framework and the system of security measures should be established by legislation.

In Zimbabwe, while the National Policy for Information and Communications Technology (ICT)[xxiii] emphasizes the significance of enhancing cybersecurity readiness, particularly by establishing cyber legislation to control cyber-related activities, a national-level cybersecurity strategy and its implementation plan are yet to be adopted.

The Government has initiated plans to establish a prominent cybersecurity leadership position tasked with overseeing national cybersecurity efforts. In this regard, per the Cyber and Data Protection Act, 2021 (37 amendments of Chapter 11:20)[xxiv], the creation of a dedicated unit named "the Security and Monitoring of Interceptions of Communications Centre" is proposed to operate under the OPC. Furthermore, the National Computer Incident Response Team (CIRT) has been assessed by ITU[xxv] but has not been created yet, and the Zimbabwe Republic Police does not have a special department or unit dedicated to cybercrime. Also, interagency coordination on cybersecurity is not yet in place. Moreover, international cooperation, including participation in international organizations and an international point of contact are not established yet.

Additionally, officials from the OPC and MICTPCS who participated in the digital governance survey pointed out the absence of cybersecurity requirements for public authorities and the identification of essential services or critical infrastructure.

Related cybersecurity legislations, policies and regulations include the Criminal Law (Codification and Reform) Act[xxvi] of 2004, Chapter VIII which defines some computer-related Crimes (Sections 162-168). Amendments to the Criminal Law made in the Cyber and Data Protection Act (Chapter 12:07)[xxvii] of 2021, this law covers some of the Budapest Convention provisions. A new Cybercrime and Cybersecurity Bill[xxviii] of 2019 contains more specific cyber-related provisions that were approved but have not been promulgated yet. National Payment Systems, Risk-Based Guideline on Cybersecurity[xxix] established in 2021, this guideline applies to all institutions licensed under the National Payment Systems, Banking and any related Acts under the Reserve Bank of Zimbabwe's jurisdiction.

3.4 Data Management, Secure Data Exchange

Data constitutes a key element of digital transformation, as every interaction in a digital setting generates data and most depend on the availability of data in digital format. Developing a digital society requires Governments to better understand what kind of data is available, both offline and digitally, and how this data can be aligned and used for creating value in the public sector and society.

Digitalization of public services means that Ministries and Government agencies capture and process data in machine-readable form. Digital transformation requires digital databases and data exchange between those. The modern digital governance model is a component-based service model, allowing the establishment of public services by reusing, as much as possible, existing service components.

In Zimbabwe, the relevant legal framework for data protection includes the Cyber and Data Protection Act, 2021 (37 amendments of Chapter 11:20)[xxx] according to which the POTRAZ is appointed as the Data Protection Authority. In general terms, the Act primarily addresses the reporting of breaches and data processing to POTRAZ, data security, online behaviour, protection for whistleblowers, data transfers, and limited data subject rights.

Most of the respondents at OPC and MICTPCS view the legal framework as adequate for the use of electronic records and electronic document management systems, while others feel the legal framework still has shortcomings and requires alignment. Furthermore, there is a need to set clear rules for the establishment of databases and the interoperability of data.

According to the digital governance survey, the use of electronic records and document management systems as well as the deployment of digital databases varies across Government institutions. For instance, land and property registers and spatial information are not yet available in electronic format, while the data in the population register and business register are partially available in electronic format. Moreover, ownership of data held by Government authorities is not always clearly established.

Through POTRAZ as the Data Protection Authority, MICTPCS is assigned as the data governance institution, but a data governance and management strategy/policy does not exist yet. Principles of data governance, including data management, data description and data quality management, are not yet clearly adopted at the national level and across MDAs.

Open data is not made available by the Government as input to service creation and public policy making. Furthermore, statistical data related to digital transformation is not always available in machine-readable format.

According to the respondents, a catalogue of state databases, services and other ICT assets is partly implemented, but regular inventories are not always properly carried

out. Most digital platforms function in silos, and lack of interoperability limits collaboration and data sharing across Government systems. The absence of a secure Government Data Exchange tool is a pressing concern, as interviewees have identified it as a critical challenge. Currently, data is exchanged through manual, paper-based systems, underscoring the need for the development of a secure digital solution for Government data exchange. Furthermore, shortcomings are also noted by respondents when it comes to supportive legislation for data exchange between Government organisations and the reuse of digitised data within the public sector.

3.5 E-identity, Digital Signatures

For digital governance services to be useful for all types of governance tasks, it is essential that the users can securely identify themselves. This requires the development of the e-identity concept and tools. This can include a digital ID or mobile ID solution together with a digital signature. Signatures must be secure enough to be recognized as evidence in court or similar situations.

The national identification system was implemented under the National Registration Act[xxxi] and in 1996, the Zimbabwe Population Registration System (an integrated computerised data system) was created to contain all biographic personal data, which is also shared for digital governance purposes. A unique persistent identifier of persons is implemented from birth, with 87.9% of the population enrolled according to the Zimstats Population Census of 2022. Unique alien ID numbers are issued to foreign residents based on the nature of their residence permits. Records in National ID are stored in electronic format. Biometric IDs were introduced in the early 2000s.

While currently e-identity system is not in place, citizens can access government e-services using the identification number from a national ID card - a card without electronic features or functionalities. Services are also available for foreign residents who have applied for their Alien ID. However, there are still other parallel identifiers in use, e.g., the national social security number. The most prominent identification methods to use digital government services include username and password, as well as mobile apps. The digital signature, along with its tools and supportive legislation, do not exist yet.

In the context of service digitization, interviewees pinpointed the absence of e-identity systems as a significant hurdle. Currently, the identification and registration of users is predominantly a manual process, requiring individuals to physically present themselves at designated offices. For instance, the Ministry of Lands, Agriculture, Water, Fisheries & Rural Developments relies on Agritex offices in different districts to register farmers by collecting their physical ID documents. Similarly, the Ministry of Local Government & Public Works handles user registration and document verification with the assistance of the Registrar General's Office. Such reliance on manual procedures highlights a clear

challenge in the transition to digital services, emphasizing the need for an integrated e-identity framework to streamline and modernize these administrative processes.

3.6 Access to Services

To be able to benefit from the advantages of a digital society, citizens and businesses should be able to access public services online. These should not simply be available, but also easy to access on different devices and platforms, inclusive and user-friendly.

The respondents to the digital governance survey consider public information to be relatively accessible via Government websites. The key sites include the Central Government Portal (zim.gov.zw), which provides access to all the Government entities' websites. The Government established a guideline for the development and management of Zimbabwe Government websites and portals in 2018.[xxxii]

The Central Government Portal also includes the ZimConnect portal,[xxxiii] which serves as a one-stop-shop for e-services delivered by the Ministries, Departments and Agencies. e-Services are accessible to both residents and non-residents after registration. Examples of e-services offered include the E-Visa[xxxiv] for online visa application, the public procurement system E-GP[xxxv] that provides access to tender notices of various Government agencies for the procurement of goods, services and construction, the E-Tip system implemented by ZIMRA to apply for vehicle Temporary Import Permits online, the E-Nurse[xxxvi] online application portal to apply for nurses training by the Ministry of Health and Child Care, the e-Cabinet process management system for the Office of the President and Cabinet, the E-Recruitment[xxxvii] provided by the Public Service Commission, among others. Several e-services are still in planning for implementation by the respective Government entities.

Helpdesk services related to public services are partly implemented and some campaigns have been held to ensure all citizens are aware of governmental digital solutions and related topics.

The digital payment system is relatively well developed, according to a World Bank study from 2021, which states that "96% of all transactions in the country are through digital means and only 4% are cash-based".[xxxviii] At the same time, according to the digital governance survey responses, the use of online banking suffers from the lack of internet connectivity. E-invoices are not yet used, neither by the public nor by the private sector.

According to respondents from the OPC and MICTPCS, work is still ongoing on the coordination and standardization of digital public services development and management. There are no central business process management rules in place yet for the development and monitoring of public services. Previously, the Public Sector Reforms and Performance Management Department used to coordinate the provision of public digital services before the establishment of the E-Government Technology Unit,

which now closely works with the Public Sector Reforms and Performance Management Department while the back-end systems are currently managed by the MICTPCS.

3.7 Digital Skills

The rapid development of digital technologies requires both public officials and citizens to acquire the skills needed to use the new tools and enjoy the possibilities of a digital society. In addition to equipping all citizens and public officials with basic skills, authorities need ICT specialists with advanced ICT and project management skills to maintain ICT architecture and support users, manage ICT procurements, and implement the Government's digital strategy.

There were 5.74 million internet users in Zimbabwe at the start of 2023 when internet penetration stood at 34.8 per cent, and 1.5 million (9.1 per cent of the total population) social media users in January 2023.[xxxix]

Zimbabwe boasts a high literacy rate of about 90 per cent and one of the best basic education access and enrolment ratios in Africa. Therefore, the country has a good education and foundation upon which digital skills training could be leveraged.[xl]

According to officials from OPC and MICTPCS who filled in the digital governance survey, the public sector understands what skills are needed for digital transformation. Although basic ICT training is provided to all civil servants through the MICTPCS and the Public Service Academy by the Public Service Commission, which runs various courses for public officials, the respondents believe that public sector officials nevertheless have insufficient digital skills to perform their daily duties. The demand is seen as huge and there are challenges, with a large share of public officials still not possessing the necessary basic ICT skills and knowledge of cyber hygiene. Furthermore, according to the respondents, capacities related to change management, business analytics, problem-solving, and critical thinking should be advanced.

The same applies to ICT staff in the public sector, with shortcomings observed, for example, in the fields of EA (e.g. TOGAF), programming, web and application development, user experience design, database management, server administration, ICT support, cloud computing, project management, cybersecurity, digital forensics, and ethical hacking.

The skills of the general public should also be reinforced. Citizens and residents are seen to have relatively good access to digital devices, although the cost of ICT devices remains a barrier. There are community information centres and kiosks in place, installed by the MICTPCS and Ministry of Finance, Economic Development and Investment Promotion. However, there are also notable challenges related to ICT equipment (or lack of it), connectivity, power, cost of data and the use of insecure poor-quality devices, which in combination lead to digital exclusion, in particular, the communication information centres do not have sufficient computers to be leveraged for digital skills

enhancement. Most of the respondents to the digital governance survey noted that more attention should be turned to the development of the digital skills of the general public and particularly to increasing the digital skills of marginalised groups who might have limited access to traditional education, such as women, refugees, elderly people, as well as SMEs.

3.8 Digital Engagement

Digital engagement is an integral part of a nation's digital transformation. The smart use of digital tools enriches and transforms existing governance models and practices, increasing the transparency, responsiveness, and accountability of Government. It also offers citizens an additional opportunity to take part in political processes, resulting in better political outcomes for society. For successful digital governance, it is beneficial to examine how it is possible to support civil society and encourage citizen engagement. This is a part of general computer literacy development.

The Access to Information and Protection of Privacy Act was passed in 2003, repealed by the Freedom of Information Act, 2020[xli] providing a legal framework for the access to information from public bodies and the regulation of mass media in Zimbabwe. Overall, the Freedom of Information Act of Zimbabwe has a significant role in promoting transparency, accountability, and data privacy. However, as cited by civil society organisations for being restrictive on media organisations, ongoing discussions and potential amendments are necessary to address concerns and ensure the Act effectively fulfils its objectives.

There is no online platform for citizen engagement and citizens have limited access to the different steps of the legislative and administrative processes via electronic channels. Citizens do not have the possibility to be engaged in the policy development process through online channels. However, a national portal where information about public procurements across the government is published has been implemented.[xlii]

There are a limited number of online tools available allowing citizens to provide feedback to the Government. No digital solutions for registering, managing and monitoring feedback from the public are in place yet.

Additionally, there is a specific new program - The Zimbabwe Accountability and Citizen Engagement (ZIMACE) in place that seeks to protect human rights and promote transparent and accountable governance across Zimbabwe by empowering citizens to hold the state accountable for its use of resources and its respect for human rights and democratic principles[xliii]. The program duration is 2023-2027.

3.9 Cooperation

To benefit from the advantages that digital governance can provide for international relations (trade, free movement, research and education, etc.), states need to take part

in international cooperation (regional or other). Such cooperation helps states to learn from one another and develop joint projects.

Representatives from the private sector, academia, and civil society are part of the Digital Economy Thematic Group and are included in the workshops organised by the e-Government Technology Unit, although according to some respondents, the cooperation could be further improved. An association of ICT companies has been established and while half of the respondents from OPC and MICTPCS see companies as interested in developing digital government services, this view is not strongly shared by others - ICT departments are rather recent at MDAs and they are seeking to keep IT-related topics contained in MDAs and the private sector engaged only through public procurements. However, there is evidence of continuously higher interest in bidding for Government ICT projects and there have been successful cases of public-private partnerships, especially concerning the infrastructure sharing policy, broadband rollout plan and the development of ICT systems and applications used in public sector institutions.

The interviews conducted revealed several cooperation examples between MDAs and other sectors - however, these examples show cooperation between government and quasi-government entities - aimed at enhancing service delivery through technology. Notably, the Digital Village Initiative stands out as a prime example of cooperation, where the Ministry works alongside Econet Wireless to enhance connectivity in rural areas. Other initiatives between central government and quasi-government institutions include the cooperation between the Ministry of Lands, Agriculture, Water, Fisheries & Rural Development and NetOne to develop an Input Management System. This initiative represents a significant step towards streamlining agricultural processes and resources.

All respondents noted that representatives of the country take part in international cooperation on digital development and agreed that the digital transformation vision and principles are aligned with international and regional standards, ensuring compatibility. Examples of existing international cooperation include a Memorandum of Understanding on digitalization cooperation between Zimbabwe and Malawi.[xli] Moreover, there is cooperation with Japan on the development of a Geospatial information database project (Greater Harare Mapping),[xlii] with China for the development of the National Data Centre (2020),[xliii] with the United States on the telecommunications infrastructure project (2020) via the Universal Services Fund, and with the United Arab Emirates, with whom the Government Experience Exchange Program is being pursued under the memorandum of cooperation agreement of 2023.

The country also cooperates with various international donors. The World Bank has run projects in Zimbabwe for decades, which included supporting the enhancement of Zimbabwe's public financial management. The World Bank also issued a country diagnostic report on the digital economy for Zimbabwe in 2021. The European Union, according to its Zimbabwe Multi-Annual Inductive Program 2021-2027, is planning activities covering "all areas of EU cooperation, including agro-food, gender, climate,

biodiversity, investment climate, digital transformation, etc.".[xlvii] In cooperation with ITU, Community Information Centres (internet access points) were established across the country between 2016-2018.

4 Situation Analysis on Enterprise Architecture

An EA is a set of tools used to plan, design, structure, and execute the introduction, modification, or analysis of the architecture of an organization. It provides a comprehensive view of the key elements and interactions of an organization's IT structure and aligns it with business strategy and objectives.

There are many architecture methodologies, models, and metamodels in use today, each with its strengths and weaknesses. It is important to evaluate the goals and requirements of an organization before selecting any approach to ensure that it is the best fit for the needs.

This chapter provides an overview of the status and practices related to EA in Zimbabwean MDAs. This part of the situation analysis directly informs the implementation of the Zimbabwe Government Enterprise Architecture (ZGEA) project by providing an overview of architecture-related maturity in MDAs.

Section 3.1 describes the ambitions and steps taken towards an EA to date, while section 3.2 provides an overview of the existing interoperability enablers, tools and solutions used in the public sector (MDAs, local governments). Section 3.3 assesses EA readiness in Zimbabwe based on a self-assessment study conducted by MICTPCS following the ACMM method, which had been commended considering that the latest version of TOGAF suggests using the Canadian Government's Business Transformation Enablement Program (BTEP) as a basis for assessment.

4.1 ZGEA Progress to Date

The Government of Zimbabwe has decided that there is a need to create a ZGEA. The main purpose of the ZGEA would be to provide connectivity, interoperability and data compatibility across all MDAs.

In 2022, the Cabinet considered and approved the Government Enterprise Architecture Framework Approach to the Modernisation and Improvement of the Government of Zimbabwe's ICT Ecosystem. A Statement of Architecture Work (SAW), Request for Proposal (RFP) and contract were formulated following the terms and structure of TOGAF®. The GoZ is not fixed on one specific methodology but is willing to combine useful elements from various methodologies that would be beneficial for the GoZ.

4.2 Enablers

4.2.1 Connectivity

In recent years, Zimbabwe has experienced significant internet expansion, with the establishment of the national Internet backbone dating back to 1997. During this period, the National Posts and Telecommunication Corporation (PTC) commenced selling

bandwidth to private Internet Service Providers (ISPs), a process overseen by the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). Among the key ISPs in the country, government-owned TelOne plays a central role by supplying bandwidth to the majority of other ISPs. The Government Internet Service Provider (GISP), operational since 1998, offers internet services to MDAs and is currently working on a government VPN network over TelOne connections. TelOne has strategically positioned Points of Presence (PoPs) in major urban centres across Zimbabwe, along the Mutare, Harare, Gweru, Bulawayo, and Victoria Falls highways, facilitating the rollout of widespread internet access within the nation.

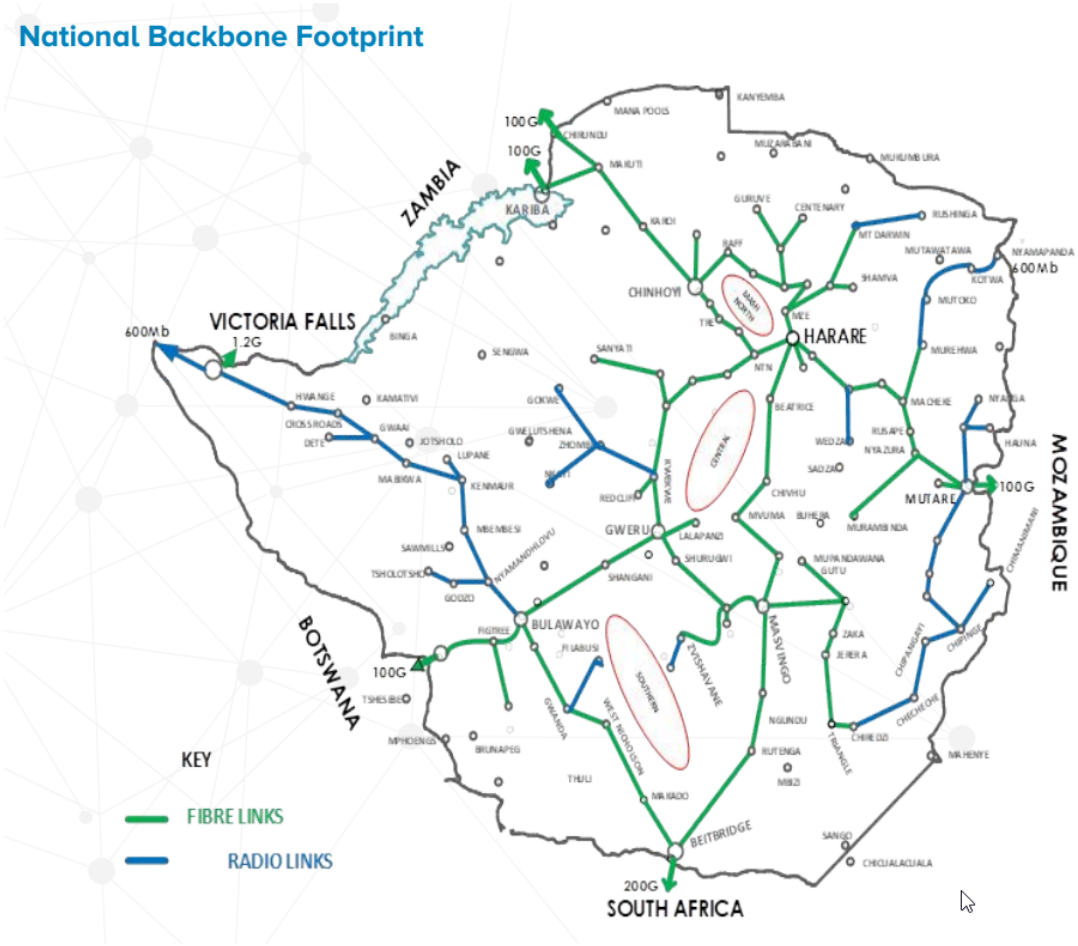


Figure 2: National Backbone Footprint[xlviii]

TelOne is grappling with legacy loans amounting to ZWL 268.4 billion (US$394m) and has been seeking debt financing to modernize its network to meet the demands of the digital economy. Unfortunately, the burden of these loans and the state of its balance sheet have hindered its ability to attract the much-needed funding. This has resulted in poor service delivery and a decline in market share, making it challenging for TelOne to compete effectively in the sector. The company is hopeful that resolving these legacy issues with the government and other financiers will reinvigorate its prospects. Additionally, TelOne faces challenges like network vandalism aimed at stealing copper,

prompting the need for upgraded fibre networks and wireless broadband LTE services as countermeasures.[xlix]

Stakeholders have expressed significant concerns about the state of internet connectivity in Zimbabwe, identifying it as a critical challenge. The inadequacy of the existing internet infrastructure not only hampers current operations but also limits the potential for future expansion and the implementation of advanced technological solutions. Moreover, the lack of technical capability and infrastructure has been recognized as a significant barrier to digitalization within institutions. While infrastructure and connectivity are concentrated in urban centres, there is limited or no connectivity in lower administrative units, with some areas still relying on 2G technology.

Moreover, outdated internet connection devices (modems, routers, switches, firewalls, etc.), often exceeding 10 years in age, pose challenges, with one Ministry reporting a 15-year-old network installation. MDAs are encouraged to use Government Internet Service Provider (GISP) services, often provided free of charge, but concerns about service quality and connection speed persist, with potential delays of up to one year for connections or upgrades. Due to resource limitations, MDAs are unable to utilize connection services from private internet service providers, although a few well-funded MDAs opt for private providers.

Furthermore, the absence of common practices for monitoring networks and responding to outages among internet service providers and MDAs highlights the need for improved incident response methods and coordination.

Currently, efforts are underway to enhance connectivity and accessibility and to extend the network to rural areas, with several projects earmarked for 2024.

4.2.2 Data Centres

The National Data Centre (NDC) in Harare, Zimbabwe, is a public asset established by the GoZ to act as a central facility accessible to all MDAs to consolidate the various disparate data centres across MDAs. The project was established under the coordination of the OPC with the MICTPCS as the technical implementing partner. Currently, the MICTPCS is responsible for the operation and management of the NDC. However, the structure for the data centre was approved under the e-Government Technology Unit and the recruitment of staff is underway with several vacancies for key NDC personnel.

The NDC claimed services include the provision of colocation services (such as storage space, power, cooling, physical security, and virtual private servers), three external network connections, as well as backup power sources in the form of generators.

In the current Harare site, there is no TIER certification, although this is planned to be acquired along with an ISO2700x security certification. The data centre uses open-source solutions for its operations and monitoring.

Additionally, there are plans to establish data recovery sites in different areas of Zimbabwe. The new locations are expected to ensure data synchronization and automatic relocation of services.

NDC services are all provided free of charge. Despite these efforts, as of January 2024, the utilization of NDC services has not yet reached 50%, highlighting a gap between the provision and consumption of infrastructure-related services.

Interviewees have highlighted several challenges within the NDC ecosystem in Zimbabwe. Firstly, there is a noticeable absence of a secure information distribution platform to facilitate seamless connectivity between the backend solutions of different MDAs - all MDAs have logically their solutions in silos without significant linking between the systems. Despite having ample resources at their disposal, some MDAs have raised concerns about the prolonged application launch times by NDC due to understaffing.

Furthermore, the promotion of NDC services and client relations appears to be undermanaged according to claims made by MDAs. NDC is reactive in its client relations and not all services are covered by contracts or have proper service-level agreements (SLAs) in place. Additionally, bringing one's hardware or software for management within the NDC is subject to additional specific requirements, and the procurement process for licenses and infrastructure can be excessively time-consuming.

As noted by interviewees, several MDAs seem to prefer maintaining their servers in their data centres rather than fully relying on the services offered by the NDC, potentially due to concerns about the reliability of the NDC's offerings and ability to respond on time to client requests. Despite these challenges, the NDC has ambitious growth plans, with investments in infrastructure and training resources. While some MDAs questioned the identity of the future clientele of the NDC, Government Policy states that all systems for MDAs must and will be hosted in the NDC once it is fully operational.

4.3 EA Readiness Assessment

4.3.1 Self-assessment by MOICTPCS

A self-assessment of EA maturity using the Architecture Capability Maturity Model (ACMM) method was conducted in May 2022 by the MICTPCS, where the Ministry was requested to honestly assess themselves.

The ACMM consists of six maturity levels and nine architecture elements. The six maturity levels show an overall level of EA maturity: none (0), initial (1), under development (2), defined (3), managed (4), and measured (5). The nine EA elements are Architecture Process, Architecture Development, Business Linkage, Senior Management Involvement, Operating Unit Participation, Architecture Communication, IT Security, Governance, and IT Investment and Acquisition Strategy. The summary of their EA maturity as they perceive it currently is presented below.

Table 1: Self-assessment by MOICTPCS using the ACMM method

Element / Maturity level	None (0)	Initial (1)	Under development (2)	Defined (3)	Managed (4)	Measured (5)
Architecture process			★			
Architecture development				★		
Business linkage					★	
Senior management involvement				★		
Operating unit participation		★	★			
Architecture communication	★					
IT security			★			
Governance				★		
IT investment and acquisition strategy					★	

4.3.2 EA Survey

4.3.2.1 Readiness for Whole-of-Government Architecture

Within digital government, the technical landscape can encompass a range of digital tools, platforms, and systems used to manage data, deliver services, and interact with citizens. It also addresses the architecture that supports interoperability among different government systems, ensuring that they can work together efficiently. Understanding the technical landscape is crucial for planning upgrades, integrating new technologies, and ensuring that the government's digital infrastructure can meet current and future needs.

Based on the EA survey filled in by 46 respondents, most of the MDAs (57%) do not currently have an **agreed architecture or a unified approach** to the adoption of technology solutions applied in their organisation.

Out of those MDAs that have an architecture or approach in place, most have been working with it since 2023. However, the methodological basis varies. Six MDAs use COBIT®, two MDAs follow TOGAF®, some MDAs noted that they used blended approaches, and one claimed they did not use any particular approach but worked based on the practical experience of their team members. Other enterprise architecture-specific architectures are used, for example for governance. *Ad hoc* architecture/self-created architecture is also used.

Different tools are used to document and maintain IT components in the MDAs. Those include technical documentation, policies and procedures, asset registers and logbooks, different databases (Oracle, Progress, MYSQL, MS Access, MS Excel, etc.) and

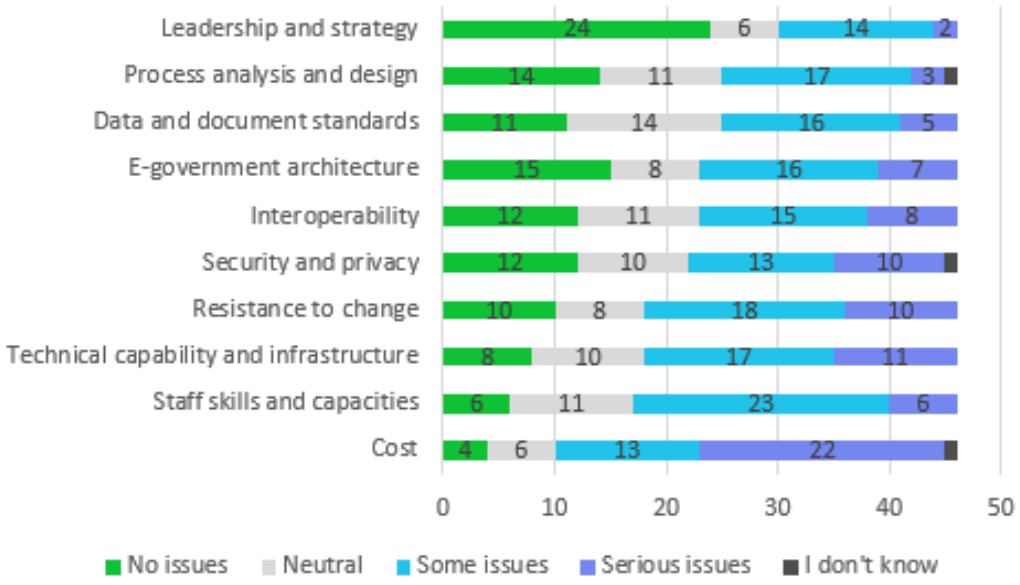
other software solutions (SAP, Jira, Document360 knowledge management platform, etc.). Seven of the 43 respondents did not mention any ICT tools being used and six of the respondents claimed no tools are in place.

The MDAs also listed the key digitalization-related **registers/systems/projects** that have been implemented or are currently being implemented in their organizations. Some examples included the online company registration, national population registration system, online border management system, national ID card system, biometric voter registration system, tax and revenue management system, e-tolling management systems, housing database, public funds management system, electronic health record, petitions dashboard, as well as internal records and case management systems, document management systems, vehicle management systems, and human resources management systems. Most of these are currently being implemented.

The frequency of **information asset inventories** also varies, with half of the respondent MDAs conducting inventories annually, a quarter of the respondents biannually, and others less frequently, except three MDAs, of whom two have live inventory systems in place and one is conducting daily updates.

Looking at digitalization at a more general level, the MDAs also indicated the main obstacles they faced within the EA survey. The main obstacles included cost, staff skills and capacities, technical capability and infrastructure, and resistance to change.

Table 2: Strongest obstacles to digitalization according to the EA survey



4.3.2.2 Readiness to Introduce Changes to Public Services

Changes to public services refer to the transformation and modernization of government services through digital means. It involves transitioning from traditional in-person and paper-based processes to online platforms that enable citizens and businesses to access

government services efficiently and conveniently. It also involves back-end integration of different government databases and systems to streamline processes and improve service delivery. The aim is to make public services more accessible, reduce administrative burdens, increase transparency, and improve the overall efficiency of government operations.

According to the EA survey, public services and relevant processes have been described in 20 out of 46 MDAs. In many cases, this is organized through internal policies and manuals (e.g. ICT policy, public procurement policy, audit policy, disposal policy, strategic planning reviews, etc.). Three responders – Zimbabwe National Roads Administration, TelOne, and Ministry of ICT, Postal and Courier Services – use Business Process Modelling Notation (BPMN).

Of respondents, 75% claimed that there is an approach in place for managing business requirements in their organisation. Examples provided included workflows and data flow diagrams (e.g. Visio), various tools and platforms (e.g. PESTLE, Tableau, Stata) as well as international standards (BPMN, UML). In addition, stakeholder interviews and workshops were often listed as process analysis techniques.

According to the respondents, business-level dependencies from other MDAs are generally understood for 45% of the MDAs. Dependencies are well known for 14% and mostly known for 18%. Some 14% said that only some dependencies are known and 9% said that they are not aware of business dependencies from other MDAs.

4.3.2.3 Readiness for Improving the ICT Development Process

In about half of the MDAs who responded to the EA survey (23 out of 44 respondents), there is no **ICT development process** in place, or they are not aware of such a process. However, 18 respondents indicated that their MDA has procedures in place for the development and maintenance of databases and information systems, eight MDAs have standard operating procedures for software development and ICT project management, one MDA uses the PRINCE2 methodology for projects, one organisation uses the Accelerated SAP (ASAP) methodology and Agile Development Methodology, etc.

Some 53% of the MDAs have standard **service-level agreements (SLAs)** or Operational Level Agreements (OLA) defined and in use. Some MDAs have SLAs with all service providers, and some with one certain technical service provider.

Around 40% of MDAs (17 out of 43) have **data standards** and **data security standards** in use. When asked about the application of such standards, four organizations noted strict adherence to the Cyber and Data Protection Act, seven MDAs referred to the application of ISO 27000 components (even if some are not formally subscribed), three MDAs made references to their organisation's ICT policy, and three MDAs noted that they apply firewalls and anti-virus software.

The EA survey also enquired about the **balance of digital and paper-based information processing** in the back office. Some 58% of the MDAs said that information processing happens mostly on paper or rather on paper. Only 7% said that it is mostly digital, and 12% that it takes place rather in digital form.

In-house teams are often deployed for IT support (81% of MDAs do it in-house), network administration (77%), project management (68%), and the maintenance of IT systems (67%). The share of using a procured partner is higher for services related to software development (62% of MDAs contract an external partner) and IT infrastructure services (43% contract an external partner and 11% use the services of another MDA).

4.3.2.4 Recommendations

Based on a thorough analysis of the current situation in Zimbabwe, the experts from eGA have put forward the following recommendations that should be considered as top-priority actions. These recommendations are crafted to address the most pressing needs for Zimbabwe and to set the groundwork for a comprehensive and sustainable transformation towards enhanced digital governance and modelling a robust WoG EA.

- As part of the WoG EA, GoZ must establish and promote **cooperation** between MDAs, to foster synergies not only within the government but also with external stakeholders, including academia, private sector entities, and civil society organizations. This collaborative approach is essential to ensure a holistic perspective and diverse expertise in addressing complex challenges and driving innovation across sectors. It could be seen as a critical aspect of making a WoG EA meaningful.
- To achieve a higher standard of governance within Zimbabwe's public administration, improving the capacity of **coordination bodies** is needed. These bodies should be adept at overseeing the compliance of systems, data, and services within the ZGEA framework and supervising their implementation. This also means that coordinating bodies are not expected to work as implementing entities, as this would create a bottleneck in the organisational model of digitalization.
- Improving **communications** is crucial to effectively engaging those affected by the process, system and structural changes created by the WoG EA. It is imperative to establish a transparent dialogue that addresses the concerns and needs of all stakeholders. This improved communication strategy should be characterized by clarity, consistency, and a two-way feedback mechanism that ensures all voices are heard and considered. By fostering a collaborative environment where information flows freely and efficiently, the government can navigate the transitions smoothly, minimizing disruption and building a resilient and adaptive community.

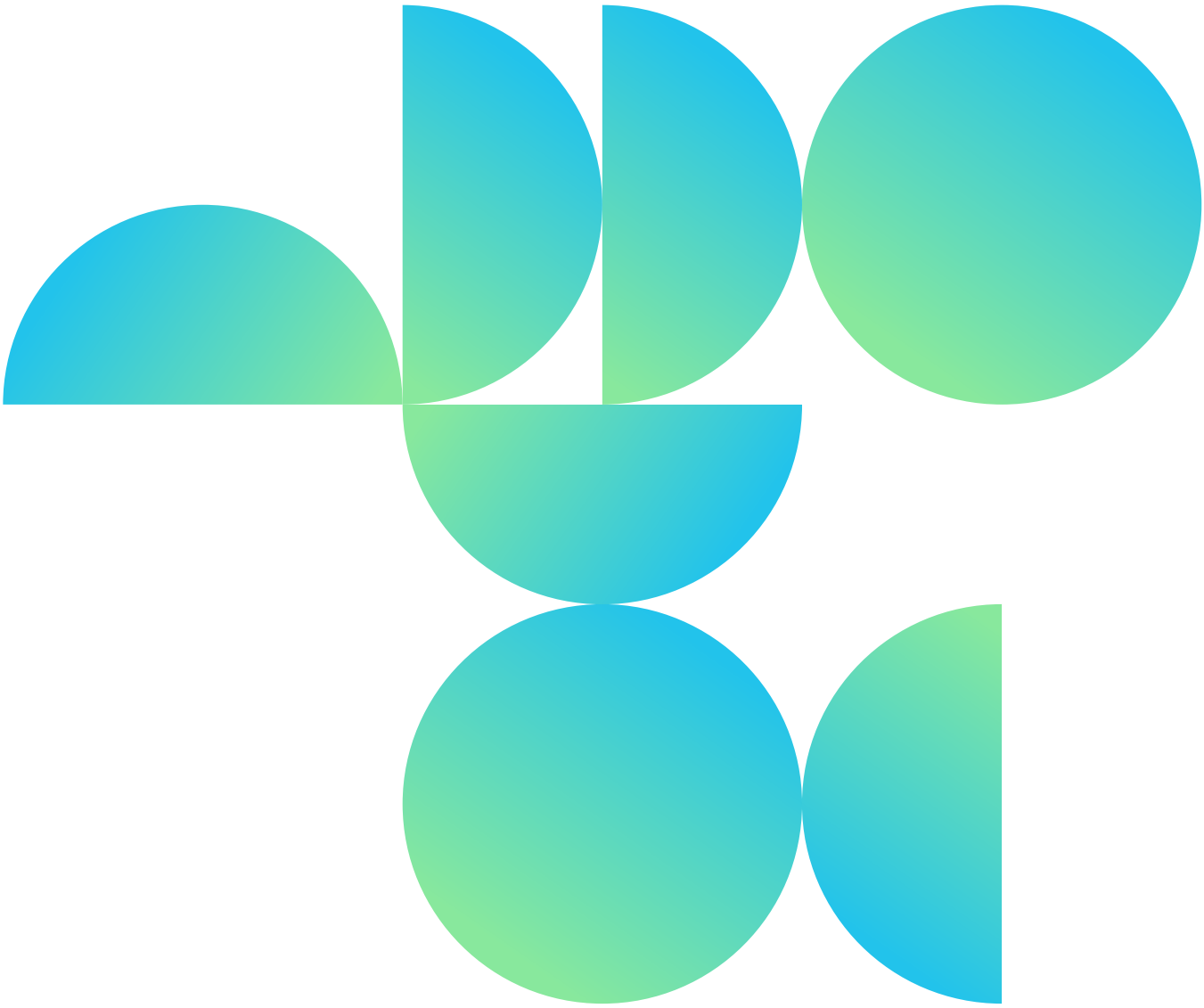
- Promoting **service (re-)design** and design thinking as part of the service development standards/guidelines is needed. The services provided by MDAs need to respond to the needs of its citizens, run as effectively and efficiently as possible considering the circumstances, and be timely and accurate with information. A user-centric approach to service design is crucial to making services more useful and usable. The WoG EA must provide a clear separation of roles and responsibilities for MDAs and how digitalization enablers contribute to providing better services.
- The need for a reliable means for connecting with other MDAs has been widely requested by MDAs. A **national secure data exchange platform** is critical and must be planned into WoG EA. Combining this with a service re-design approach is expected to deliver quick wins for GoZ.
- MDAs have significant concerns about the discoverability of information and data assets in the public sector. To facilitate interoperability and data exchange, it is essential to carry out a comprehensive **inventory of state databases**, information systems, and information assets. This ability of discoverability - if not implemented as a one-time inventory but rather a repeatable systematic process - serves as a key step towards ensuring that government entities have a transparent, current, and detailed understanding of the various types of data and their contents that are maintained across public institutions. The execution of this inventory will enable a more coherent approach to data management and support the government's ability to make informed decisions.
- The creation and implementation of a **digital identity ecosystem** is a transformative step towards modernizing identity verification and access to digital services. This is typically a challenging task as it has a direct impact on society and must be accepted by society both at the citizen and service provider levels. It is important to start working on this early on to ensure that all non-technical issues can be handled timely.
- A citizen-facing **front-end approach** must be agreed upon and implemented. There are alternatives from technical (responsive web, mobile app, website, kiosk, etc.) and organisational (portal, network of interoperable front-end solutions, domain-based self-service environments, etc.) perspectives. Defining a unified way of how a wide range of services are delivered to citizens allows one experience for citizens and provides a safe environment for MDAs to plan their citizen-facing developments.

References

[1]The World Factbook (2023). Zimbabwe.
[2] The World Bank (2022). GDP per capita (current US$) - Zimbabwe.
[3] World Bank (2021). Access to electricity (% of population) – Zimbabwe.
[4] World Bank (2022). Individuals using the internet (% of population) – Zimbabwe.
[5] World Bank (2022). Fixed broadband subscriptions (per 100 people) – Zimbabwe.
[6] World Bank (2022). Mobile cellular subscriptions (per 100 people) – Zimbabwe.
[7] United Nations (2022). UN E-Government Knowledgebase – Zimbabwe.
[8] United Nations (2022). UN E-Government Knowledgebase – Zimbabwe.
[9] Transparency International (2022). Corruption Perceptions Index - Zimbabwe.
[10] ITU (2020). Global Cybersecurity Index.
[11] National Development Strategy 1, 2021-2015.
[12] Transitional Stabilization Program 2018-2020.
[13] Zimbabwe vision 2030.
[14] Zimbabwe Situation (2021). ICT Masterplan to guide industrialization.
[15] National Health Strategy 2021-2025.
[16] POTRAZ Strategic Plan 2019-2023.
[17] African Wireless Communication (2023). Zimbabwe gains National Broadband Plan.
[18] Electronic Transactions and Electronic Commerce Bil (2013).
[19] Chronicle (2021). Cabinet approves Electronic Transactions and Electronic Commerce Bill.
[20] Access to Information and Protection of Privacy Act (2003).
[21] Freedom of Information Act (2020).
[22] Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ).
[23] Zimbabwe National Policy for Information and Communications Technology (2016).
[24] Data Protection Act (Chapter 11:22) (2021).
[25] CIRT assessment for Swaziland, Liberia, Zimbabwe and Congo, 10-14 March (2014).
[26] Criminal Law (Codification and Reform) Act (2004).
[27] Cyber and Data Protection Act (Chapter 12:07) (2021).
[28] Cybercrime and Cybersecurity Bill (2019).
[29] National Payment Systems, Risk Based Guideline on Cybersecurity (2021).
[30] Data Protection Act (Chapter 11:22) (2021).
[31] National Registration Act (1976).
[32] Guidelines for the Government of Zimbabwe Websites (2018).
[33] ZimConnect for e-services.
[34] E-Visa.
[35]E-GP Portal.
[36]E-Nurse.
[37]E-Recruitment.
[38]The World Bank (2021). Digital Transformation a Key Enabler of Long-Term Resilient Growth in Zimbabwe.
[39] Data Reportal (2023). Digital 2023: Zimbabwe.
[40]World Bank (2021). Digital Economy for Zimbabwe, Country Diagnostic Report.
[41] Freedom of Information Act (Chapter 10:33) (2020).
[42] Zimbabwe e-GP Portal.
[43] DAI (2023). Zimbabwe Accountability and Citizen Engagement (ZIMACE).
[44] TechUnzipped (2023). Zimbabwe and Malawi Sign MoU on Digitalization Cooperation.

[45] Japan International Cooperation Agency. The development of a Geospatial information database project (Greater Harare Mapping).
[46] DCD (2021). National Data Center in Zimbabwe Opens.
[47]Zimbabwe Multi Annual Inductive Program 2021-2027.
[48] TelOne Integrated Annual Report (2020), page 8.
[49]TelOne Annual Report (2022), page 18.

Delivering a seamless Government experience



D2-1 Legal Review and Recommendations

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

1 Purpose of the Document

Regulation of technologies should be agile. The focus should be on what is done and not on how – using which technology - it is done. When digitalising governance, existing law can remain largely valid and there is no need for a lot of specialised legislation. Detailed law on technical matters risks becoming obsolete quickly. Digital is a format, a tool, to be included in the general legal and administrative processes to make administration and business more efficient while securing the rights of individuals. At the same time, the absence of clear rules means a lack of legal certainty. It is important to ensure that the new way of doing things fulfils the aims of existing legislation. For successful digitalisation, it is essential to include relevant legal issues early in the development process.

The project "Whole of Government Enterprise Architecture Modelling for the Government of Zimbabwe" includes a legal and regulatory review consistent with the scope of the enterprise architecture. The Terms of Reference (ToR) stipulate that this shall include a "review of legislation and regulations to identify any articles that may hamper the function of interoperability or in general impede the enterprise architecture because they are outdated, or stipulate requirements that are counter-digital or that impede digital activities". In addition to reviewing existing instruments, essential missing rules shall be identified. The ToR lists topics that should be included: digital interaction with the public sector, inclusion, and rights; cybersecurity; procurement; data collection, -sharing, -minimization and open data; interoperability and data registries; cloud computing; digital by design; digital documents, identities, and signatures; access to information; e-commerce; privacy and data protection. Furthermore, the evaluation of cybercrime law is indicated as a separate task.

This document contains the legal review and related recommendations that form part of the project "Whole of Government Enterprise Architecture Modelling for the Government of Zimbabwe". The recipient of the document is the e-Government Technology Unit, in the Office of the President and Cabinet.

2 Scope of the Review

The main partner for the work is the e-Government Technology Unit in the Office of the President and Cabinet (OPC). OPC has developed a set of enterprise architecture principles, which are relevant for the legal review as they should be reflected in and supported by legislation. The principles are interoperability by default; data minimization (including the once-only principle); designation of core data registries; trustworthiness, confidentiality, and security of data; user-centricity; availability of a service catalogue; resilience of the digital government; and validation and compliance mechanisms.

The list of issues and legislation to be covered is long and comprehensive. Although the scope of the project does not permit a detailed analysis of all possible related laws and regulations, a general analysis has been made and the key issues related to the overall project scope identified. The work has been carried out through analysis of legislative acts and in-person discussions with many stakeholders. The OPC e-Government Technology Unit enabled successful meetings with stakeholders and provided invaluable support during the legal expert's visit and in online meetings before and after. In April 2024, the OPC e-Government Technology Unit presented a 'Memorandum of Principles for the e-Government Act', intending to reform the institutional structure within the OPC and the entire Government at large for dealing with e-Government and digitalisation. This Memorandum is still within the internal development process and comments to it concern the initial draft version.

3 Validity of Digital format

Although there is normally no need for a lot of specialised legislation for digital issues, certain matters must be clear in law. This includes the validity of the digital (or other electronic) format of decisions, declarations, or other documents as well as the validity of digital identities and signatures. Now there is no specific legislation on this in Zimbabwe. It is possible to presume legal validity without it being specified in law, by treating the new, digital format as just another version of documents or signatures. This was suggested by some interlocutors. However, this approach lacks legal certainty. It can be useful temporarily to allow moving forward in the absence of legislation, but the more the digital format starts being used, the more problematic it will be if there are no clear rules. A lack of legal certainty is known to deter investments as well as to reduce trust among people.

This means that the adoption of either a law on digital transactions or such provision in some other law is a matter of priority. In 2013 a bill on Electronic Transactions and Electronic Commerce was presented, which has not been enacted and there does not appear to be any new draft nearing adoption. A law including updated parts of this bill could plug gaps and ensure legal certainty, although much of the text from 2013 is obsolete by now. The delay in the legislative process should not mean that no action is taken, pending the adoption of an entirely new law. Many laws allow Ministers to prescribe matters by regulation. It is important to achieve legal clarity on the validity of the digital format, but the exact way this is done has some flexibility, which was confirmed by interlocutors pointing to different options (inclusion by interpretation, regulations, legislation brought to Parliament by a Minister rather than the Attorney General's Office, etc.).

It was observed that the Attorney General's office, especially the drafting department, was seriously understaffed and overworked due to understaffing. It was not possible to find out about the status of the draft Electronic Transactions Bill, but stakeholders were informed that the process had been drawn out, with many questions and debates. Normally, the legislative process includes one workshop after the preparation of a draft by the Ministry and Attorney General's Office. In the case of the Electronic Transactions Bill, there have been at least four workshops, and the draft has gone back and forth to the responsible Ministry several times. Once a draft does come to Parliament (for which no timeline exists in this case), it is assumed that the bill will have to be 'unpacked' into components and discussed with MPs in workshops. As the digital skills of MPs vary a lot, their ability to assess the bill will also vary.

Legislation should deal with legal recognition of electronic communications and writing and the legal effect of electronic signatures. Rules on originals and copies are one of the small but important clarifications needed in the digital society and that applies to many different laws and situations. It is good to deal with private and public electronic

transactions in the same manner and to have one electronic (digital) signature for both sectors. However, legislation with many separate issues in one law where the only uniting factor is that electronic tools are used (as was the case with the 2013 bill) can be unnecessarily cumbersome. Another aspect that should be updated in any new version of the bill is to oblige or at least encourage the use of electronic communication and prohibit the setting of additional criteria for doing so, to encourage e-Governance. As laws like the Freedom of Information Act already explicitly recognise intangible formats of information, it is possible to move ahead with such format also awaiting a law on electronic transactions, but support by some form of legal acts will ensure legal certainty.

The proposed e-Government Act does not aim to replace general legislation on digital transactions but aims to create an organisational basis for dealing with the digitalisation of public administration and to delineate roles, responsibilities, duties and powers of participants within the e-government ecosystem as well as to promote digital solutions.

4 Digital identity and signature

Digital signature and identity are a key issue for e-governance and one of the few issues that need special legislation. Zimbabwe currently has no law on the issue, with the above-mentioned 2013 bill having contained both useful and somewhat dated provisions, but none of which have been enacted. On questioning the Ministry of Home Affairs and the Civil Registry Department their readiness for the introduction of a digital ID, they replied that they are not yet ready but working on it. What needs to be examined is its usability i.e. where such an identity would be used and how.

Digital identity legislation should contain provisions on secure electronic signatures and certification authorities with some detail on what type of signatures to use or reference to a body that can issue regulations. People need to know that the way they provide their signature or prove their identity will be accepted by administrative authorities and courts. One system that can be used in all contexts (public and private) will permit society to reap the benefits of the reform. It will also have the potential to be popularly accepted if people can use the same system for all relevant purposes (like for public services as well as banking and signing private documents). A user-friendly system is normally also legally more secure as people are less likely to look for shortcuts or abuse the system. A digital identity needs to be based on a secure identification of the person so that it is known that it designates one specific person and that person alone. In Zimbabwe, the Civil Registry is in quite good shape but there are unclarities regarding for example people who left the country decades ago but still exist in registries, therefore parallel to the digital identity, work on organising the Registry should continue.

Recognition of digital format includes that the laws accept digital (or other electronic) signatures, as mentioned above. Validity can be stipulated in a special law or for example an administrative code or similar. What is essential is that whenever a law mentions signatures, this can also be digital so that there is no risk of courts or authorities rejecting digital signatures. It is not necessary to add these words in every law, which would be a cumbersome process and create risks of loopholes if it is made clear somewhere that this is the case.

In those cases where electronic identification is currently used in Zimbabwe, like the electronic case handling system, identities are created for that specific instance. A signature consisting of logging in via e-mail and signing in the system exists, or it is possible to print, sign on paper and scan. Only about 1% of signatures are made by the electronic in-system means. The system is created only for the case management system, and it does not have any additional means to verify the identity of the signer. Regular personal e-mails are used for notifications and other communications. The lack of security of regular e-mail communication has been raised on several occasions in different contexts over the past years, but the practice largely continues. There is a lack

of awareness of how electronic identities should be used even among parts of the administration, where staff share passwords and access online resources with the same identities.

Zimbabwe takes part in Pan-African work (with 47 countries, under the auspices of the African Union) to create an ID for Africa. The work is mainly under the Registrar General, also the Postal and Telecommunications Regulatory Authority (POTRAZ) and its data protection unit have been incorporated into this work. The Pan-African ID serves as a travel document and is machine-readable, however, it does not contain a chip and the cost of adding that is at the moment prohibitive.

As part of the current government enterprise architecture project, Terms of Reference for a Foundational Project relating to digital identity have been developed. This foundational project is expected among other items to refine and elaborate legal aspects of the matter.

5 Data Protection

Zimbabwe passed a Cyber and Data Protection Act in December 2021, which entered into force in February 2022. The Act establishes a Cyber Security Centre as well as a Data Protection Authority, although its content is mainly aimed at data protection. Some stakeholders criticized that the law deals insufficiently with cybersecurity and in fact, the inclusion of these words in the title is partly due to a mistake: the initial draft contained more cyber issues and when it was changed the name change was not dealt with at the proper time. The stated aim of the Act is to create a technology-driven business environment and encourage technological development and the lawful use of technology as well as to reform the Criminal Code and increase cyber security to build confidence and trust in the secure use of information and communication technologies.

The Data Protection Authority under the law is POTRAZ, where a distinct unit has been created. It has the competence to investigate data protection issues of all organisations, including ministries and other authorities. The unit was initiated in February 2022 when a first circular on the appointment of data protection officers was issued. The unit was staffed and fully operational in May 2023 and conducted a snapshot survey on awareness of data protection soon after initiating work. Citizens were to some extent aware of their rights but only about 27% knew data protection. Since then, POTRAZ online awareness programmes have been popular and successful, as people have after this made complaints to the authorities and these have been on adequate and proper matters. As for compliance by companies regarding the appointment of data protection officers, only about 35% are deemed to be complying at the time of the visit (March 2024). Almost 95% of companies have asked POTRAZ for training. The first train-the-trainers programme was launched in April 2024 and interest is very large. POTRAZ is aware of the need to find solutions that balance business needs and data protection – given the novelty of the rules, this is a work in progress.

POTRAZ is in the process of creating a register of all data processing companies in Zimbabwe. Compliance has so far been based on encouragement of voluntary compliance and awareness raising, with no fines issued although the authority has powers to impose fines. Alternative dispute resolution has been used and has been sufficient, with no need for POTRAZ to initiate court proceedings, for which it also has the powers and competence. There are several initiatives of international cooperation to study best practices and learn from countries in the region that have started implementing rules earlier. The notion of privacy by design is something that is just entering the discourse and not yet much used.

In the Act, definitions of data subjects, controllers, and so on, in general, follow international practice. The Act only applies to data using automated means, which is a pity as it is better to have technology-neutral legislation. The key to protection should be the content of data and not its form. Apart from this, most provisions follow

international best practice. There are rules on the quality of data, proportionality and purpose for data processing, the distinction between sensitive and non-sensitive data, as well as on duties of the data controller and rights of the data subject. Although the grounds for data processing are like those of the EU General Data Protection Regulation, largely seen as setting out international best practices, the approach is somewhat different. Consent is the basis and other grounds are exceptions, while in the GDPR different grounds are at an equal level and especially for the public sector, other grounds are in practice more common than consent. There is a possibility for implied consent for non-sensitive data of adults, which GDPR does not permit. The possibilities of processing sensitive data even without consent are quite wide-ranging, mentioning scientific research and certain types of organisations of public interest. For such use, a requirement of anonymisation should apply but this does not appear to be the case in this Law. There are however some safeguards, and secondary legislation should set stringent rules.

In line with the GDPR, there are special provisions for decisions taken based solely on automatic processing, which the data subject can refuse. However, in addition to consent for such decisions, they can also be based on law in which case the right to refuse shall not apply. Transborder flows of data are regulated in a manner in line with international standards. Also, the public sector still needs to adapt to data protection legislation as provisions on data handling are extra challenging when the number of data subjects handled is very large. There is a lack of awareness among public servants on data protection, for example data shared between different levels or departments of an institution without awareness that there may be restrictions for this. The current legal as well as institutional framework is in place, but this is recent, and awareness-raising is still needed.

POTRAZ as a whole and the data protection unit made a very good impression. The awareness and knowledge of salient issues are present as well as plans for how to continue improving the situation. The Human Rights Commission can also have a certain role in the context and both this organisation and POTRAZ thanked OPC and the project for inviting them to a joint meeting so that all sides could hear one another and establish contact. The only potential risk in the data protection context now appears to be the data protection unit becoming overwhelmed, unless they can increase the number of employees.

6 Registries and Archives

Stakeholders expressed the view that a leap forward in digitalisation could be achieved if the Civil Registry, the Company Registry, and the Deeds Office were digitalised. The idea of key registries and non-duplication has not been implemented yet. Some interlocutors said that 'people also need to be interoperable', pointing to a lack of coordination between different ministries or agencies. There is a need to determine where data should reside and who is responsible for databases. Several different bodies are mandated for data collection, which needs to be clarified to have the 'once-only' principle. At the moment, data is not in a standardised format and even if some differences can be allowed, some standardisation needs to be decided. Such issues need legal support.

6.1 Civil Registry

Although the Civil Registry in practice already operates like a key registry, there is no legal provision specifying this or what this means. Now there are one-on-one contacts between the registry and other counterparts in an ad hoc manner regarding providing access. The legal basis for giving access to registries and databases is often unclear. The question of which ministry or agency should initiate work on providing access is also not clear, with the Ministry of Justice presumably having a key role but this Ministry is not being active or very responsive regarding digital issues. The Civil Registry used to be a pioneer in automation and a model that others studied but this is no longer the case, with later developments having been slower. The basic responsibility for data (for which the Ministry or Authority is responsible in each case) must be clear in law. In many instances, this may follow from existing laws on different issues, where someone is designated to compile and maintain registers, but any gaps need to be identified and in the practical work of interoperability, relevant parties need to be aware of such rules.

6.2 Archives

The current Archives Law is from 1986 and thus not in line with digital archiving. Principles for digital archiving have been prepared and presented and legal amendments are in the (early) process of amendment. The digital awareness of the personnel dealing with archives, at least at the higher level, is good. At the same time, the supporting legislation as well as the practical systems are still inadequate as these are based on paper-based archiving. The question at what point a transaction becomes valid when there is no paper record is currently not based on clear rules but rather on the interpretation of rules. Given the rapid development of technologies, the systems used for archiving and similar present a challenge, as entities may be paying for systems that they do not use, as these are outdated but procurement was such that they are locked into the system.

One of the challenges due to lacking updated legal framework is that there are no rules on disposal of digital archives. There have been instances of poor handling with people disposing of hardware that potentially contains sensitive data. There is an urgent need for legal provisions on this. The law should deal with data and not its format so that the rules are the same across the board, but the current rules only suit paper-based data. As for the situation at the moment, much is down to the discretion and decisions of individuals in ministries, departments or agencies.

6.3 Digital Data

There are some issues of records being in poor order, so organising data in any format needs to take place so as not to create a digital mess. The Company Registry is in quite good order so it would be possible to integrate it into an interoperability system, even if there are gaps in the digitalisation of old documents, from the 1950s for example. Records e.g. the Civil Registry have not yet fully been digitalised. In this process questions on the correctness of data come up, for example regarding persons who may have left the country several decades ago but whose data was not updated. In urban areas, digital data is already largely used (for personal documents of different kinds) but this is not the case in rural areas. There is a lack of funds and manpower to introduce the technology. This is partly mitigated by mobile sub-offices and citizen support centres. However, some fears were expressed that if people need assistance from such concentrated places, this could open a window for corruption. Another challenge is proprietary systems for storing data, where government data may become inaccessible if licence fees are not paid on time – opening for a potential abuse by the licence holders. The idea has been floated that the government should commission software made specifically for it.

7 Digital Rights and Access to Services

The readiness of people in Zimbabwe to use online services varies regarding the availability of devices, access to the internet and digital skills. Quite a lot of people are familiar and comfortable with online, especially mobile solutions but a large proportion of people do not have access neither to devices, or the internet. Even many lawyers and other professional persons lack computers and in public service, it is common that many persons must share the same device. There are also limits on how electronic payments can be made. Several stakeholders pointed to the need to ensure secure and accepted payment possibilities as something that may delay the provision of electronic services.

Awareness of digital rights is gradually improving, at least with awareness-raising on data protection. The Human Rights Commission has so far not dealt much with digital issues, but the recently launched Integrated Electronic Case Management System (IECMS) led to complaints regarding access to justice. This issue was raised by many stakeholders as highlighting the kind of (legal) problems that e-services can lead to. Many interlocutors agreed that the readiness of people was not properly assessed. The Integrated Electronic Case Management System was introduced by the Judicial Service Commission in 2022 and rolled out in steps during 2022-2023. The system includes virtual hearings and other court processes. The document handling uses scanning and uploading and not digital documents (which do not exist yet in the country). Nevertheless, the process has not been successful and as legislation eliminated other, physical ways of conducting cases, the system entailed problems with access to justice. Many people are not ready to use the new system, there are problems with infrastructure including poor connectivity or lack of devices as well as insufficient competence to use these properly. The problem is exacerbated by the fact that not only do individuals lack the required means to use the electronic system but also smaller courthouses and administrative offices, especially in rural areas, are poorly served. As the system is supposed to handle all sorts of cases, this includes cases of parties that may lack financial and other means to get assistance. While such a system may be suitable for business-related cases, the Human Rights Commission mentioned how in cases of parental support for children the parties may be indigent. Given that other ways of dealing with cases are no longer supported by legislation, this has created practical and legal problems. The various support mechanisms are seen to have been inadequate.

Basic legal preconditions for electronic work are at hand in the form of most case law and statutes existing electronically. Rules on evidence and similar are applied regardless of format, which is in line with best international practice and avoids the need for lots of specialised legislation that furthermore may become obsolete. However, many lawyers as well as some judges, prosecutors and others still prefer to use hard copy legal texts even if the Ministry of Justice, Legal and Parliamentary Affairs ensures that soft copies are available for all relevant instances. Even among lawyers, a vast majority

do not have their personal laptops and even though courts made rooms available with access to computers and the internet and there are support centres, the transition to the new system has been problematic. Access to justice is a fundamental right, which includes both the right to be able to bring cases and present oneself and to observe court cases. Given problems of internet access, live YouTube feeds and similar are not easily accessible or adequate.

As for a broader transition to electronic services, the Public Service Commission is aware of the challenges of new technologies and has taken this into account in its work for some time. Modelling exercises have been conducted on what the changes mean both regarding implementation and utilisation of technology and administrative as well as legal questions. For pensions and human resources, several processes have been digitalised. In the absence of a secure digital identity, potentially useful steps like remote interviews and electronic contracts are hampered as it is not possible to verify identities. One concern is possible redundancy due to jobs disappearing and although to some extent this can be dealt with by relocating people, this may not be possible if major reforms are introduced, which can cause problems with labour law. The resistance to change among public servants and the ethics of pushing for faster and larger changes than what people are comfortable with is another challenge.

Current legislation on a range of issues can present problems for going digital if the law prescribes that everyone should get some document, and if someone does not have access to the internet, it is unclear if an electronic version would be enough. One example mentioned was the idea of electronic payslips. The law prescribes that everyone should have access to a payslip. If this forces people to buy devices, it can be questioned if this violates any law, quite apart from whether people would be satisfied with a 'payslip on demand' or the possibility of going to a Community Information Centre. If the law stipulates the 'old' requirement with no exceptions, legal challenges to new processes are possible. These are the kinds of obstacles that can only be addressed through a comprehensive review by legal experts on different issues.

The Public Service Commission provides training for raising digital skills, with tailor-made courses requested by different entities. To deal with problems of accessibility as well as lack of digital skills, the Judicial Service Commission has established service kiosks at court centres. There are also Community Information Centres and training programmes, with experts going around the country and training local officials. Disused post offices and other buildings belonging to ZIMPOST can be used for this purpose, including supporting potential bidders for public procurement to use electronic tools. These are examples of practical measures to allow the use of electronic means even without the population having the means to directly use these.

Legislative changes aiming at increasing the ease of doing business were introduced in 2015-2016 allowing some digital tools, but even after such legislation was introduced, many processes remain analogue. New changes came in 2019-2020 for example to the

Companies Act but although at were quite clear (digital records and archives, digital payment systems, etc.) not all of this was achieved.

Currently, digital data exchange takes place based on agreements between parties for a specific case, but the overall recognition of the digital format is not clear. As part of the current whole of government enterprise architecture project definition of requirements for a data exchange platform is in scope. It is expected that this future foundational project will also deal with the legal aspects of data exchange in more detail.

8 Access to Information

Zimbabwe has a Freedom of Information Act from 2020, which applies to information in all different forms recognising the digital format. It stipulates that requests shall be made in writing in the prescribed manner, so relevant secondary legislation must be adopted to make sure that the 'prescribed manner' is the easiest possible electronic one. More efficient administration thanks to digitalisation will permit reduction in the periods for responding to requests. Even without full digitalisation, the periods in the law (21 days with a possibility of extension) are excessive, as public information should be rapidly available. The forms of access listed will be largely obsolete, as one of the most noticeable benefits of digital governance is the ease with which information can be shared. The Act does not include proactive sharing of information with the public.

It is good to have freedom of information and access to information legislation that applies to all forms of information, electronic or other, but when the digitalisation of administration has proceeded, it is important to evaluate both the legislation (including guidelines and other secondary legislation) and the practice, to ensure that the benefits of new ways of sharing information are used to the full extent. Currently exchanging information is mainly done manually. Provisions still exist in regulations on things like how different copies of documents shall be distributed, even colour-coding copies for different purposes. The uncertainty on what such rules mean in a digital world means that many officials prefer hard copy documents simply as the rules for these are clearer.

Public servants sign a confidentiality obligation by which they commit to upholding the Official Secrets Act, which is generic regardless of the form of data. This is taken seriously by all sides as there have only been a few cases of breaches; in the instances where people have been dismissed for violations, this has been upheld by courts, which indicates that the matter is not used spuriously by employers. As for data protection as a more recent issue, sensitisation is a work in progress in cooperation with POTRAZ.

9 Digital Evidence

In many countries, the judicial sector can become a bottleneck for digitalisation, when courts demand traditional, paper-based evidence. Legislation in Zimbabwe has been updated so that electronic format is admissible, and the value of electronic evidence is recognised as equivalent to paper through amendments to the Criminal Procedure and Evidence Act adopted through the Cyber and Data Protection Act of 2021. Legislation explains what search and seize means, what provisions there are for service providers and others to keep data and how hosting providers must act to rapidly remove illegal content. Caching and hosting providers have different specified liabilities and responsibilities. The capacity to deal with digital evidence is improving but still a work in progress including the possibility to preserve digital evidence. Cooperation with service providers (private firms) does take place but is often slow. If phones are to act as trusted devices for carrying out digital services and identification, there is a need for improved routines on how to react quickly to thefts, cloning and so on. Operators do not want to be identified with crime so although they comply with court orders, it is more difficult to get proactive cooperation.

The Integrated Electronic Case Management System means that judicial staff in Zimbabwe have some experience with electronic issues (although normally scanned paper documents rather than digital ones) but this does not mean that all judicial staff feel comfortable with the new format. Judges tend to be sceptical about training, so it is important to tempt them to learn more about data protection and cyber issues in a way that suits the profession. POTRAZ has had some success in its interactions with the Law Society of Zimbabwe and the Judicial Services Commission, sharing international and regional experiences (e.g. from Malawi). Service of court papers can be done via e-mail, which has raised questions about the security of regular e-mail and the possibility of reaching people securely, as not everyone has e-mail accounts or regularly accesses these even if they have an account.

10 Cybercrime

People globally have started using digital tools at a much more rapid rate than that with which their skills and awareness has increased and many problems of cybersecurity, including cybercrime, are global. In Zimbabwe cybercrime has been included in the criminal code, modified by the Cyber and Data Protection Act 2021. Including cybercrime in the criminal code rather than in a special law is good as general provisions of criminal law can apply. As all countries, Zimbabwe is faced with challenges due to the international nature of cybercrime, the ease with which borders can be bypassed and difficulties in identifying the culprits. Such issues cannot be dealt with by drafting laws but require international cooperation and training of the relevant officials.

Stakeholders in Zimbabwe pointed to challenges for law enforcement due to lack of skills among staff and the rapidly evolving cybercrimes, often of an international nature. An additional challenge is that some specialised software and equipment are under sanctions and thus will not operate in the country, including surveillance equipment. The police feel underequipped. However, training programmes are ongoing, with international help in some cases. For example, 1700 police officers have been trained on AI with the support of the United Arab Emirates, Egypt has supported cybercrime training and training cooperation with POTRAZ exists. The capacity of the police is improving but it is a work in progress. The efforts include working with crime prevention.

Legislation on cybercrime largely exists. Given the rapid development, there are issues missing, like cryptocurrency or AI related rules. However, in general there is a legal basis for dealing with different types of cybercrimes. Police and prosecutors have dealt with some such crimes and have persons who are familiar with the questions. At the same time, neither organisation has dedicated departments or personnel just for cybercrime and especially in smaller locations in the country, the preparedness is not good. Often smaller stations lack connectivity so even the technical means are lacking – added to which officials have limited competence. The general population also lacks awareness, which makes them vulnerable to cybercrime and means that people may not be aware of how and when to report crime.

Identity-related offences are included in the law. Cases of identity theft have so far been few in Zimbabwe but there have been some cases of hacking and using credentials of prominent people as well as some extortion cases. Preparedness for dealing with an increased use of digital identities is increasing but still incomplete.

Cybercrimes mentioned in the law include hacking; unlawful acquisition of data; unlawful interference with data, data storage or with computer systems; unlawful disclosure of data code; unlawful use of data and devices. Other crimes may have cyber elements. Penalties are potentially severe. The aggravating circumstances mention e.g. such matters as interfering with aircraft through the data related crimes. There are offences relating to electronic communications and materials, including sending

threatening data messages and provisions on cyber-bullying. In conclusion, cybercrime legislation is recently updated and in line with international best practice, even if rapid developments mean it needs to be under constant attention.

11 Cybersecurity

Cybersecurity illustrates the horizontal nature of digital issues as it concerns all areas of society, and it is crucial to address cybersecurity risks and to ensure that these are understood and considered throughout the administration. Security aspects must form part of considerations regarding working methods, technologies, service provision and so on. It is an issue that is included in many different areas of law. International best practice is reflected in international conventions and model laws (SADC, African Union).

POTRAZ has established a Cyber Incident Response Team (CIRT) managed by its data protection unit. The Cyber and Data Protection Act stipulate that there shall be established a unit in the Office of the President, which shall be called the Cyber Security and Monitoring of Interception of Communications Centre. This is still in the process and many interlocutors pointed to its need, even if quite good mechanisms exist for cooperation between institutions on cybersecurity matters, to the extent that Interpol has positively assessed Zimbabwean efforts. POTRAZ is proactive in threat investigation as opposed to what is the norm for traditional regulatory activities (which are reactive). Knowledge-sharing platforms and transparency are important tools to mitigate the effect of incidents that are almost inevitable to happen. Sensitization is still needed among companies regarding what assistance can be given and how to deal with incidents.

With the setting up of the Cyber Security and Monitoring of Interception of Communications Centre there are amendments made to the Interception of Communications Act. Although in some circumstances, all countries can monitor communications, this should be an exception to the general protection of privacy of communications and cybersecurity needs do not change this. The Centre shall be the sole facility through which interception shall be authorised and it shall also act as an advisory body on cybersecurity issues. If this is a professionally staffed body that sees its tasks as safeguarding rights of individuals in the digital society, this can be a positive development. However, it must then have the kind of competence that is found in courts – meaning judicial competence. As the members are to be appointed by Ministries and different authorities, it does not appear as if the judicial competence is a criterion. Decisions of interception must be very restrictive and taken only on legal considerations with no room for political decisions. As an example, a similar provision to that found in the Anti-Corruption Commission Act could be used. It is stated that a requirement is that a member is eligible to be appointed as a judge or has been a judge of the High Court or Supreme Court of Zimbabwe (even if that Act allows some deviation from this rule).

12 Communications Legislation

A well-functioning and well-regulated market for ICT is a prerequisite for digitalisation. Zimbabwe has a Postal and Telecommunications Act from 2000, amended on some occasions since. The regulatory authority is POTRAZ. Universal service provisions and a system for licensing exist, in line with international practice. ICT legislation is important for cybersecurity as this is a tool for making demands on different actors in the field. Some modern elements of ICT legislation have not been fully included in the Zimbabwe law, like online communications and the level of responsibility for different sector participants –mere conduit, caching, and hosting. The Telecommunications Law is in the process of reform and although the bill has not yet been made public, it was mentioned that the amendments deal with incorporating such ICT-related amendments. POTRAZ appears to be a well-functioning and competent authority, dealing with the relevant questions in line with best international practice.

There are three main mobile operators. Coverage is quite good but there are pockets of problems. There are also issues with many counterfeit or old handsets and problems of affordability both of devices and of connectivity. The latest available ZIMSTAT figures for 2022 state that about 50% of the population has internet access at home, our interlocutors mentioned now about 71%, but due to difficult terrain there are remaining areas that can only be covered with difficulty. There are efforts, supported by law, to ensure colocation, sharing of infrastructure and such means to enable covering more areas. Only a small section of schools nationwide has internet access and problems of access were mentioned for courts, hospitals and other places. The government has plans to increase this as well as to provide free Wi-Fi areas around clinics and hospitals, but these plans are quite far from completion. Devices are quite expensive in Zimbabwe and about 50% of internet users use smart devices. Digital skills vary a lot and even among frequent users with modern devices, the awareness of risks is often low. However, the Ministry conducts digital skills programmes, and the situation is improving.

13 Procurement

Procurement legislation was amended in 2018 by the Public Procurement and Disposal of Public Assets Act. The Act allows the use of electronic tools. A portal has been created for procurement projects. This portal is now the way procurement is handled although the fully electronic procurement system is still in the process of development. It would be greatly helped by interoperability with the Company Registry and Civil Registry as this would facilitate checks on shareholders, board members and other company info that is needed. At the moment the checks are made manually. Regulations have been developed and submitted to the line Ministry but need to go from there to the Attorney General's office.

The procurement office uses electronic means to quite a large extent. This permits things like encrypting tender documents that are only decrypted on the day of opening the tender, thus limiting corruption. An electronic identification system with unique keys and encryption has been developed for the procurement system, for registered entities. It is only possible to use the system after registering and obtaining such an identity, used only for this system. Online payments are possible within the system, by using bank cards or mobile electronic payment systems (EcoCash/OneMoney). Such payment systems can be used within the procurement system, for some local payments and in some other cases.

Companies are largely interested in the system and willing to use it, as it facilitates for them and their interest is to be able to win contracts to the maximum extent at good conditions, so they are willing to invest in being able to use the system. It has been more challenging to get procuring entities onboard, as here resistance to change is demonstrated. Currently, there are attempts to persuade entities to come onboard but if this does not work, regulatory and practical means to enforce compliance may be needed. The Government has introduced so-called performance contracts for state companies and parastatals to ensure compliance with different rules, including using the proper procurement system.

There were some different opinions expressed concerning procurement, with some criticism of the slowness in a fast-moving technology world, where what is procured may no longer meet needs. At the same time, others (also OPC) pointed out that ministries and authorities have a responsibility in the process to be proactive and cancel or amend anything that is no longer suitable, not expecting the procurement authority to be able to do this as they cannot have the detailed knowledge of needs across the administration. Legal departments of Ministries are often inadequately represented in the procurement process, so systems have been developed or procured that do not meet legal requirements. The Ministry's legal departments tend to deal only with contractual issues and do not get involved or are not competent in evaluating the way systems will be used and how this relates to the Constitution and laws.

14 Consumer Protection and e-Commerce

There is a Consumer Protection Act from 2019 that sets up a Consumer Protection Commission. The Act contains definitions of consumer and other relevant general issues. Electronic transactions are included in the law. As the Minister can give policy directions and as there is a special commission, it should be possible to take care of any special e-commerce-related issues. The data protection unit cooperates with the Consumer Protection Commission as well as the Competition and Tariffs Commission. There is no specific e-commerce legislation, but such legislation is not necessary if there are other legal acts dealing with pertinent issues, like how to identify oneself, the safety of payments, consumer protection and competition issues.

15 Remarks on Regulatory Environment

Many commentators voiced the view that what is lacking in the country is a designated entity that oversees proactively dealing with legislation and regulations, making sure that necessary steps are taken to adjust to the digitalisation process. Ministries initiate legislation in their different areas of competence, while the coordinating task could be for the drafting department of the Attorney General's office, which however is seriously understaffed and has no specialists for digital matters. The crosscutting and interdisciplinary nature of digital issues is a challenge in all countries. In Zimbabwe, government business tends to be governed by regulations regarding the specific services that are not suitable for crosscutting digitalisation issues, which require a new way of cooperation.

The legislative process in Zimbabwe contains several steps such as public consultations, deliberations in the relevant portfolio committee and legal committee in the Parliament including verification of the constitutionality of any proposals. Depending on the nature of comments and when these are made proposals can be amended or stopped. Various viewpoints and checks of the suitability of the proposal are included in the process, but this does not solve the issue of delays in preparing the legislative drafts, where the overworked and understaffed Attorney General's Office presents a bottleneck. There are some quicker ways to adopt new rules in the form of statutory instruments, if Ministers push for this, and it is permitted to engage external drafters so with political will, there may be ways to adopt the needed laws quite quickly.

Plans for digitalisation including a Digital Transition Framework from 2018 have been adopted. This was the basis for the Judicial Services Commission for how they went digital and if different organisations used the same framework, there should not be problems with digitalisation and with interoperability. Stakeholders however pointed to inadequate and very different understanding among different public bodies. The recent proposal for an e-Government Act and a different organisational set-up within OPC aim to strengthen the role of the coordinating body by creating an e-Government Technology Agency that although being part of the OPC, will have greater autonomy. A strong body dealing with digital issues within all government structures is a positive development. Its role and competence must be set out in law so that there is no question of its ability to make binding decisions. At the same time, the role must be delimited so that it does not lead to excessive centralisation. The Agency should deal only with matters necessary for the functioning of cross-cutting ICT issues and interoperability and not infringe on the substantive work of Ministries, Departments and Agencies. The policy-making role of the Ministry of ICT, Postal and Courier Services and its relationship with the Agency needs a firm legal basis.

16 Recommendations

- The priority areas for future legal work should be drafting support to the Attorney General's office on an electronic transactions law (or legislative changes to other laws to this effect) to ensure that the legal validity of the electronic format is recognised and specifically to ensure legal support for electronic identities and signatures.
- The legal aspects of digital identities/ are included in the foundational project.
- Key registries should be identified with clear rules on responsibility for gathering and keeping different types of data and identification of organs with basic responsibility for the data. A general legal framework should provide a clear understanding of how to determine the authentic and sole controller of data as having multiple controllers for the same dataset is a factor slowing down digitalization and interoperability efforts.
- Parallel to creating a digital identity, work on organising the Civil Registry and Company Registry should continue to ensure a proper basis for the new identity format.
- Data protection is well handled in law and with a competent agency, which however is very new and likely to face a heavy burden in implementing and awareness-raising.
- In different cases the law stipulates requirements adjusted to a paper-based system so legal challenges to new processes are possible. A comprehensive legislative review by legal experts on different issues should be conducted, to identify and deal step by step with arising questions.
- Digital evidence is recognised by law and increasingly accepted in practice.
- Cybercrime legislation is recently updated, in line with international best practices, even if rapid developments mean it needs to be (globally) under constant attention and improvement of knowledge and capacity must be ongoing.

16.1 Proposed Steps

16.1.1 Short Term

- Strengthen the coordinating function of the e-Government Technology Unit to enhance ICT governance across all MDAs.
- The most immediate concern for the project is to ensure greater legal certainty on the validity of the digital format, which concretely can have three components of work:
- Adoption of regulations or other acts to clarify what is already possible to assume (and that is supported by the intangible format being recognised in

law) that digital documents, decisions etc. are legally valid. Use can be made of legal possibilities for Ministers to adopt regulations in quite a short time.

- Support the Attorney General's office with the drafting of (more comprehensive) legislation on digital transactions including digital identities (and including promoting the use of the digital format), alternatively outsource drafting work.
- Inclusion of legal provisions in the proposal for a digital identity.
- Review the procedures for search and seizures as well as the cooperation model between the different stakeholders (government and private companies) to improve routines on how to react quickly to thefts, cloning etc.

16.1.2 Medium and Long-term

- Ongoing legal (and administrative) analysis to identify possible legal unclarities or obstacles shall be an ongoing task in all ministries, departments and agencies supported by advice from OPC.
- Constant attention to cybercrime and cybersecurity issues but no specific project-related activities were proposed.
- Continuation of the good work on sensitisation of data protection issues and adoption of guidelines, etc., but no specific project-related activities proposed.

D2-2

Drafting Support to the Government of Zimbabwe for Digital Transactions-related Legislation

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

1 About the Document

Part of the legal task in the project "Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" is to draft terms of reference for a legal professional or firm to perform any legal revisions which may be needed. This work shall consist of drafting support for necessary legislation related to the validity and use of digital (electronic) transactions in Zimbabwe. The legislation shall support the creation of the Zimbabwean Whole of Government Architecture (ZWoGA) and electronic service provision.

Content of the document:

1. Background: context for necessary legal changes, including
   1.1. Current situation: A brief overview of the present circumstances, highlighting general challenges.
2. Objectives and statement of work.
3. Expected tasks and outcomes: Description of expected activities and deliverables including expected timeline.
   3.1. Expected qualifications of the consultants.

2 Background

For successful e-Governance, it is essential to include the relevant legal issues early in the development process. This does not mean the need to draft a lot of specialised legislation for digital issues, as specialised law may create parallel systems with different rules for the same service or the same data depending only on the format or technology used. When new and complex technologies are introduced and data is kept in a new and intangible format, it may appear as if rules and regulations should mirror the complexity and provide special provisions for all innovations. This is not the case, but instead, it is important to ensure that the new way of doing things and the new technologies used can fulfil the aims of existing legislation and that there are no obstacles in law to the new methods. If obstacles are encountered, these can usually be abolished by fairly limited legislative amendments, but if there is not sufficient attention paid to the issues early on in the reform process, the negative consequences can be serious.

Laws on administration, business and various rights of individuals already exist and can keep fulfilling their role even if the way things are done has changed. Organisations can keep their role but someone needs to have a clear mandate to deal with common issues that arise because of interoperability. At the same time, there are also legally relevant things that are different, for example, what decisions look like and how they can be kept or how people identify themselves and sign things. Thus, several issues need to be addressed in law.

Legislation should be written in a general manner so that it can cover many different specific situations and remain relevant for a long time. This principle has become ever more important with rapid technological development. Legislation that is not technologically neutral risks becoming obsolete quickly. If the detail is needed on technical or practical matters, this can be in other types of legal acts that can be amended more easily and that can contain more descriptive language, like guidelines, regulations or similar. The law should provide basic rules plus the mandate for a suitable body to adopt the secondary legislation as well as implement laws and other rules, to make the law effective.

2.1 Current Situation

Zimbabwe has adopted or amended several legal acts, which are relevant to the digitalisation process and e-Governance, in recent years. These include:

- Cyber and Data Protection Act 2021
- Freedom of Information Act 2020
- Criminal Law (Codification and Reform Act), amendments by the Cyber and Data Protection Act 2021 (regarding cybercrime)

- Interception of Communications Act, amendments by the Cyber and Data Protection Act 2021

Through these Acts as well as regulations and other forms of instruments, a basic legal framework exists for dealing with digital data and various forms of electronic services. To some extent, it is possible through the interpretation of legislation to include new formats of signatures and documents.

However, what is missing is a coherent legal framework that provides for the legal validity of the digital format of documents, decisions and similar. A Bill was presented in 2013 for an Electronic Transactions and Electronic Commerce law, but the law was not adopted and work with the Bill although reportedly ongoing is without visible progress in recent years. Partly, the Bill has become obsolete and partly issues included in it (electronic commerce consumer protection) have been adopted through other legislation (the Consumer Protection Act, 2019). What is still needed includes the legal recognition of electronic communications and writing and the legal effect of electronic signatures. Rules about originals and copies are examples of small but important clarifications of law that are needed in the digital society and that apply to many different laws and situations.

It is good to deal with private and public electronic transactions in the same manner and to have one electronic (digital) signature for both sectors. However, legislation with many separate issues in one law where the only uniting factor is that electronic tools are used can be unnecessarily cumbersome. Legislation should encourage the use of electronic communication and limit the possibility of demanding additional criteria for doing so. A requirement of traditional format should only be made when objectively necessary. It is not incompatible with the electronic form to have a requirement of notarial confirmation or similar, as this can be a step to verify or approve an electronic transaction. The evidentiary weight of electronic transactions should not rely on printouts needing 'paper' affidavits and similar. The same is true for the production of documents and information.

Digital Signature and Identity are a key issue for e-Governance and one of the few issues that needs special legislation. The relevance of signatures in the legal sense is that it is a way in which an identified person declares something – thus, legally the digital aspects of signatures and identities can be dealt with together.

Other issues related to electronic transactions that may fit better in other legislation than in a general electronic transaction law include the retention of records. This is a question that should depend on what these records are, what is their content and for what purpose they are kept. The duty for telecommunications service providers to keep records should be in the law for such services and specified in licences. Caching, hosting and mere conduit rules are normally found in telecommunications (ICT) legislation and the relevant law in Zimbabwe is currently in the process of amendment.

To sum up the key points:

- There is a need for a law that ensures the legal validity of the digital format.
- There is a need for legislation on digital identities and signatures, linked to the creation of a Digital Identity/Signature. Details should be in secondary legislation.
- If laws already exist on transactions, a new law on digital transactions should only deal with those aspects that are different because of the new technologies.

3 Objectives and Statement of Work

The objective of the project is to provide legislative drafting assistance to the Ministry of ICT, Postal and Courier Services/e-Government Technology Unit in the Office of the President and Cabinet (OPC) to draft the required legislative provisions, in the form of a Bill for a Digital (Electronic) Transactions Law (or legislation of another name with the relevant content) and/or additional legal amendments to other legislation.

The legislation shall be presented as a Public Bill in the form of a Government Bill. The legislative process includes the Cabinet making a policy decision, which may be initiated by a proposal by the minister in charge of the relevant issues, following which the minister is directed to prepare a bill. The proposed principles of the bill are sent for review to the Cabinet Committee on Legislation (CCL). The drafting is normally done by the Legal Drafting Department in the Attorney General's Office. Any draft Bill shall be considered by the CCL and may be sent for approval to the Cabinet or entered directly into the legislative procedure in Parliament.

The Attorney General's Office does not have adequate capacity and expertise in all different subjects. Due to a lack of resources, there are delays with legislative drafting as evidenced e.g. concerning legislation on digital transactions. There is a possibility to use outside assistance in the form of outsourcing legislative drafting work to experts. To facilitate and expedite the drafting of key legal provisions of digitalisation and e-governance, external legislative drafting assistance is needed.

The key beneficiary and client will be the Ministry of ICT, Postal and Courier Services as advised by the e-Government Technology Unit under OPC. The e-Government Technology Unit under OPC will support the vendor by providing up-to-date information about the proposed e-governance structures and digital services as well as any other relevant information on existing or planned digital transactions.

1. The vendor will collaborate with the Ministry of ICT, Postal and Courier Services and with the Office of the President and Cabinet to obtain the information needed to be able to propose legislative changes.
2. The vendor will deploy an expert or a team of experts.
3. The expert(s) will work from their workplace, using their equipment, unless required to be present on official premises for access to a specific material or similar.
4. The vendor will be informed through the Office of the President and Cabinet about the work and progress on digital identities and signatures as well as on digital service delivery, prepared through separate projects, to be able to coordinate with these projects.
5. The Office of the President and Cabinet will be the vendor's main counterpart and point of contact and will facilitate the contact of the vendor with the relevant

MDA. The Office of the President and Cabinet will organize the provision of essential facilities for the work, including access to relevant stakeholders.

6. The expert(s) will report directly to the Project Lead in the Office of the President and Cabinet and seek concurrence from that Office on key project deliverables.

4 Tasks and Deliverables

4.1 Task #1: Analysis of the current legal situation

During this phase, the Vendor's team will:

- Study the existing legislation in Zimbabwe that is relevant for e-Governance and digital transactions, including studying any existing draft Electronic Transactions Bill and the process related to this Bill since the first presentation of a Bill in 2013.
- Identify relevant gaps or obstacles to transition to digital services and digital format of data and transactions. The legal review and recommendation produced as a deliverable under the project "Whole of Government Enterprise Architecture Modelling for the Government of Zimbabwe" may be used as a basis for the work.
- Propose key issues that need to be included in new legislation and propose the structure of such legislation – specific law(s) or amendments to existing laws.

Requirements for the analysis:

1. The result of the analysis shall be presented logically and simply, focusing on key issues and explaining why the legislative change is needed.
2. All texts must be in good and clear English and as short as possible.
3. The analysis shall be discussed with the key beneficiary/client before moving to the legislative drafting stage.

4.1.1 Deliverables under Task 1

Analytical Report.

4.1.2 Expected timeline for Task 1

Delivery of report: four weeks from the start of the Project.

Discussion with beneficiary: within one week of delivery of the report.

Finalisation of the report: within one week after discussion with the beneficiary.

4.2 Task #2: Legislative drafting

During this phase, the Vendor's team will draft legal text in the format and amount proposed by the Vendor and decide together with the beneficiary under Task 1. It is assumed that the deliverable will be a Bill of a Digital Transactions Law, but the parties may decide to instead propose amendments to existing legislation or to propose more than one new law.

4.2.1 Deliverables under Task 2

Draft legislation in a format ready to be entered into the ordinary Parliamentary legislative procedure.

4.2.2 Expected timeline for Task 1

Delivery of draft legislation: six weeks from the end of Task 1.

Discussion with beneficiary: within one week of draft legislation.

Finalisation of draft legislation: within one week after discussion with the beneficiary.

4.3 Total project timeline

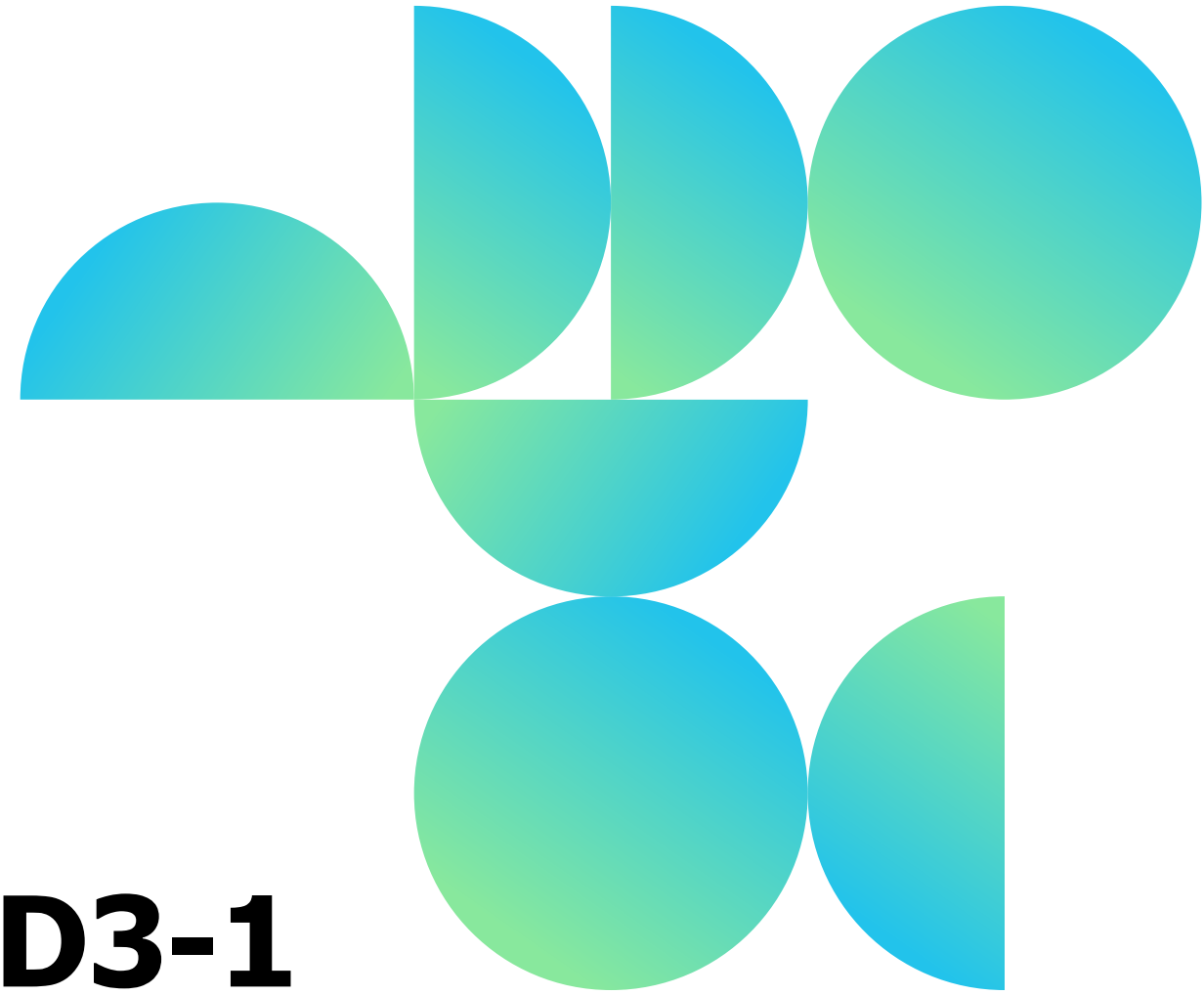
Fourteen (14) weeks from project initiation to closure.

4.4 Expert qualifications

The Vendor shall be an individual legal expert or a team of legal experts/law firm. The expert(s) shall have the following competence:

1. Knowledge of the Zimbabwe legal system including the legislative process.
2. Experience in legal drafting (in the form experience of drafting legislation, regulations, and other forms of binding or non-binding instruments or decisions).
3. Excellent English language skills.
4. Understanding of digital services, interoperability of data, data protection, digital signatures and related issues.
5. Demonstrated experience in delivering results on time and to a high-quality standard.

Delivering a seamless Government experience



D3-1

EA Approach and Framework

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Acronyms

Acronym	Description
ADM	Architecture Development Method
BTEP	Business Transformation Enablement Program
EA	Enterprise Architecture
GoZ	Government of Zimbabwe
ICT	Information and Communication Technology
MDA	Ministries, Departments and Agencies
MHTESD	Ministry of Higher and Tertiary Education, Innovation, Science, and Technology Development
MOHA	Ministry of Home Affairs and Cultural Heritage
MICTPCS	Ministry of Information and Communication Technology, Postal and Courier Services
OPC	Office of the President and Cabinet
PSC	Public Service Commission
TOGAF	The Open Group Architecture Framework
WoG	Whole of Government
WoGA	Whole of Government Architecture used as synonym to ZWoGA
ZWoGA	Zimbabwean Whole of Government Architecture, used as synonym to WoGA.

1 Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the "An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for enterprise architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to enterprise architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

The Enterprise Architecture Approach and Framework document is oriented toward the team responsible for preparing and running the architecture development process - not the architecture implementation process. It is expected to be a small team that runs the architecture work preparation led by an experienced enterprise architect, who needs to prepare and run the architecture work.

The document should be used as a baseline to guide the team in preparing and steering the architecture process. The team should revise the methodology and adjust it according to the specific needs of the expected architecture iteration.

It is essential to monitor that the approach handled by this methodology should be covering the whole of the government. To ensure that all stakeholder's interests would be covered, and the development of architecture would be balanced.

2 Framework

This chapter provides an overview of the environment where the Enterprise Architecture (EA) methodology and work fits in. The Whole of Government Architecture (WoGA) is a mechanism to identify and describe changes to government operations where ICT capabilities are included to solve challenges identified by the administration and society. Therefore, the architecture framework must be in the service of public administration in general and it must be aligned and adopted with other strategic processes in the public sector.

2.1 Tactics

EA is a discipline usually executed by architects where business context and technical implementation aspects are modelled into one holistic view. The work has several significant contextual constraints that must be addressed by how the EA is defined and implemented:

- **Whole of Government** - The Government of Zimbabwe (GoZ) has embarked on the exercise to define and describe the enterprise architecture for the whole of government. This requires repositioning EA terminology and work into a generic work where each stakeholder and entity internally are left intact.
- **Skills and experience** - as the list of stakeholders is large and EA must be understandable for the stakeholders then each EA iteration must adapt to the current level of skills existing (baseline) and as part of the capacity building plan it must allow the creation of necessary skills for next iterations of EA (target). Also, the experience of stakeholders is a significant contributor. This means that additional complexities related to EA must be included in future versions with the growth of experience among stakeholders.
- **Repeatability** - as the engagement of stakeholders, communication of ICT governance and architecture-related skills are not strong the establishment of the architecture with one go is questionable. WoGA should be developed iteratively to allow necessary complexity to be built into it over iterations and make the WoGA into a persistent discipline.

These context elements are considered when defining the approach constraints in the following chapter. Additionally, it is recommended to periodically self-assess the situation from the perspective of transformation enablement. This is refined in more detail below in the chapter BTEP Assessment.

The context for architecture must be (self-)assessed at the beginning of each iteration of the process to identify current circumstances and obstacles that will require changing the process.

2.2 Custom Methodology

The original requirements of the project (Terms of References) suggest that the architecture should be based on vocabulary based on TOGAF® Architecture Development Method (ADM). Additionally, the workshops conducted in Harare in January 2024 indicated that stakeholders contributing to the work are biased towards the TOGAF world. This can be seen as a recommendation toward using TOGAF as the baseline for ZWoGA while keeping other approaches on the radar and using pieces of those to enhance the Zimbabwean-specific methodology.

For that reason, to make the architecture development sustainable for the long term the Zimbabwean Whole of Government Framework and Methodology should be seen as simplified TOGAF where some elements have been added to address local requirements. This allows to use a TOGAF-based skillset in combination with local situation assessment to be used for improving the methodology.

Considering future improvement to the methodology - as among the stakeholders and potential users of the architecture there are various backgrounds and experiences - it is recommended to align the complexity of the architecture and its methodology so that a strong majority (about 80% of stakeholders) would understand the ideas described in the architecture. Making it too complicated will push stakeholders away from the whole process and therefore would be counterproductive.

Use TOGAF as the baseline while monitoring other methodologies for good examples and artefacts to incorporate into the Zimbabwean WoGA methodology.

Making the ZWoGA too specific for high-level and well-educated architects' risks that many users of the ZWoGA will not understand the content and therefore the ZWoGA will be left unused.

The initial methodology for ZWoGA is described in the chapter 3.

2.3 Formatting and Notation

During workshops in January 2024 as the initial exercises related to EA a set of architecture description languages was introduced. Considering the large set of contributors to the EA model and an even larger set of stakeholders who must align the work in their MDA into the context of EA, it is important to keep the modelling language at the simplest level. Therefore, the least-formalised box-and-line modelling style is recommended. Once a good baseline is established by the stakeholders and readers some more formal architecture description languages could be gradually introduced.

Use box-and-line description language for diagrams and model views.

2.4 Scope

Defining a Whole of Government Enterprise Architecture defines a strong need to rationalize what will be the smallest objects that the architecture should reach. Typical alternatives would be to look things down to the ministerial level, MDA level or specific department (responsible for public service) level.

Considering the size of the public sector in Zimbabwe and various levels of digitalization in the MDAs the preferred details should be kept on the MDA level.

This is recommended for the following reasons:

- Ensures technical alignment between a multitude of organisations.
- Preserve autonomy in the MDAs to create the most effective information systems.
- Potential legacy issues contain the problems at the MDA level without impacting the whole of the government.

The whole government approach implies further constraints for the work. The most notable that must be considered are:

- **Stakeholders** - every MDA is an independent stakeholder in the EA process while hiding its internal structure and relations from the EA discussions.
- **Ministries** can add further constraints and elements in their domain to be adopted by MDAs in their domains, but Ministries cannot dismiss any aspects of WoG EA inside their domain.

- **Coordination** - relying on the independence of each stakeholder the coordinating entities are expected to use EA to define "how" MDAs cooperate, while "why" and "what" of the cooperation will be left to the specific MDAs and domain-based projects.

Considering the currently available skillset in GoZ it is recommended not to overload the EA (and its methodology with external references - like EIF, GovStack, GERA etc.) as this would raise the entry level for many stakeholders too high. It is recommended to start with the architecture from a perspective that is understandable and acceptable to stakeholders at their current level of competence. With the following iterations (where the complexity of architecture also rises) it is reasonable to bring in other references and frameworks along with relevant training and capacity-building activities.

2.5 Approach

Architecture should be developed iteratively while keeping a long perspective on the horizon.

Architecture must be developed iteratively.

Figure 3 presents the context for an architecture development iteration and presents its cyclical nature. The size and scope of the architecture iteration should be defined through implementation constraints.

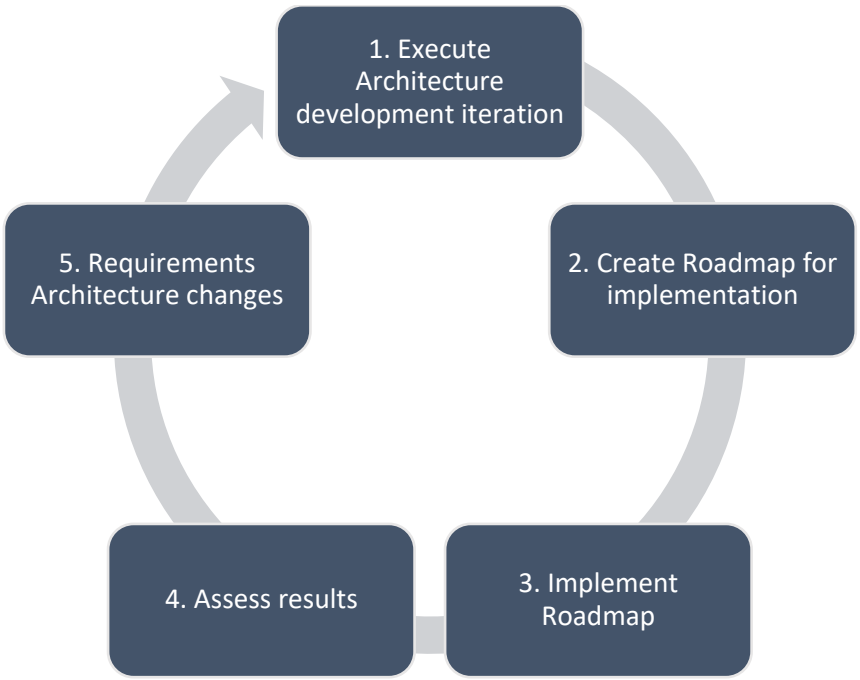


Figure 3. Architecture development iteration framework

The framework steps are explained below.

1. **Execute architecture development iteration** - The architecture development step (according to methodology defined in the current document, see chapter 3) where architecture is developed and described. The result is a target architecture description and a list of necessary changes to reach a desired future vision state.
2. **Create Roadmap for implementation** - Changes are arranged into a Roadmap which should be at least at the granularity of 6-month cycles. With this step architecture work is handed back to stakeholder organisations as the implementation plan must be composed considering stakeholders' actual capability for implementation. This requires also assigning relevant resources for necessary changes to become implementable.
3. **Implement Roadmap** - Implementation of the Roadmap with a yearly (or other agreed interval) validation of the progress.
4. **Assess results** - assess the intermediate result of architecture implementation considering: (a) the initial vision/goal of the architecture, (b) actions implemented according to the roadmap, (c) obstacles discovered during implementation and (d) changes in the world/environment (including new expectations in the public sector and society but also emerging technologies). If the architecture vision/goal and Roadmap are relevant continue to the next steps in the roadmap (go to step 3).
5. If it has emerged that architecture goals/vision is not relevant any more define the change expected. **Prepare initiation of a new iteration** of the whole of government architecture - continue at step 1 and assign a core architecture team for that. See chapter Changes for Next Iterations about initiating the next iterations.

2.6 Engagement

The inclusion of all the stakeholders in the architecture creation process has been one of the expectations in Zimbabwe. As the Whole of Government EA is foremost an agreement process for aligning perspectives of the stakeholders this requirement presents some issues. Experience of the EU and countries of significant size demonstrates that the agreement process takes a lot of time when there are too many participants. This creates the challenge of working effectively - without the agreement any tangible deliveries are impossible - and balancing it with the inclusion of all/most stakeholders.

Additionally, the process of agreeing on the architecture and making changes to the architecture is expected to repeat and therefore some sustainable approach must be defined to be effective in the process also in the long term.

The recommendation is to develop architecture in two steps:

- Architecture is developed by a working group that is composed of critical stakeholders. The architecture working group assigned for this will engage in this step.
- The wider set of stakeholders (or in future iterations other interested parties from the public and private sectors) will review and comment/validate/approve the proposal of the working group.

2.7 BTEP Assessment

To understand if, when and for what the architecture definition work must be (re-initiated) the BTEP assessment methodology should be used.

The method used for the MICTPCS self-assessment in 2022 was the Architecture Capability Maturity Model (ACMM) method, which was used in older versions of TOGAF. The latest versions suggest using the Canadian Government Business Transformation Enablement Program (BTEP).[1] Therefore, this chapter presents an updated version of the self-assessment, which has been conducted by the BTEP factors. The updated assessment was informed by the results of the two online surveys as well as the knowledge gained during the practical workshop. The updated assessment will be reviewed together with the stakeholders in the following phases of the project.

Figure 4 BTEP Overview

BTEP uses a Readiness Rating Scheme that can be used as a starting point for any organization in any vertical. Each one of the readiness factors is rated to:

- **Urgency**, whereby if a readiness factor is urgent, it means that action is needed before a transformation initiative can begin.
- **Readiness status**, which is rated as either Low (needs substantial work before proceeding), Fair (needs some work before proceeding), Acceptable (some readiness issues exist; no show-stoppers), Good (relatively minor issues exist), or High (no readiness issues).

- **The degree of difficulty to fix** rates the effort required to overcome any issues identified as either No Action Needed, Easy, Moderate, or Difficult.

Table 3 Self-assessment result at the beginning of 2024 architecture development iteration.

#	Readiness factors	Description	Urgency	Readiness status	Degree of difficulty to fix
1	Vision	Ability to clearly define and communicate what is to be achieved in both strategic and specific terms.	Yes	Acceptable	Moderate
2	Desire, Willingness, and Resolve	Willingness to achieve results, accept consequences, and stay committed to the task.	Yes	Good	No action
3	Need	Specifying what the organization can't do without it and what it will enable the organization to achieve.	No	Fair	Moderate
4	Business Case	Concrete benefits that the organization is committed to deliver and goals that the organization is committed to achieving.	No	Fair	Moderate
5	Funding	Clear source of fiscal resources that meets the endeavour's potential expenditures.	No	High	Easy
6	Sponsorship and Leadership	Keeping everyone "on board" and focused on the strategic goals.	No	Good	Easy
7	Governance	Ability to engage all parties with an interest in or responsibility to the endeavour, ensuring that the corporate interests are served, and the objectives achieved.	Yes	Fair	Moderate

#	Readiness factors	Description	Urgency	Readiness status	Degree of difficulty to fix
8	Accountability	Assignment of responsibility, recognition of measurable expectations by all parties.	No	Good	Easy
9	Workable Approach and Execution Model	An approach that makes sense relative to the task, with a supporting environment, modelled after a proven approach.	Yes	Fair	Difficult
10	IT Capacity to Execute	Ability to perform all the IT tasks required by the project, including the skills, tools, processes, and management capability.	No	Acceptable	Moderate
11	Enterprise Capacity to Execute	Ability to perform all tasks in areas outside of IT, including the ability to make decisions within tight time constraints.	No	Acceptable	Moderate
12	Enterprise Ability to Implement and Operate	Ability to absorb changes arising from implementation and to operate in the new environment.	Yes	Fair	Moderate

3 Methodology

The architecture work - as an iterative process - is cyclical (also presented above in the approach description). The current chapter provides insight into a recommended methodology for architecture definition work for the government of Zimbabwe. The methodology described here was guiding the work during the first iteration of the 2023-2024 work moderated by e-Governance Academy (eGA). This methodology is loosely based on TOGAF ADM but has been adjusted for circumstances in Zimbabwe. Considering the TOGAF analogy the architecture definition work relates to TOGAF ADM steps A to F (architecture vision, business architecture, information system architecture technology architecture, opportunities and solutions, migration planning) although those have been restructured to have a better match with the whole of government approach in Zimbabwe.

The phases related to architecture governance (steps G, H) are to be considered as routine work of entities responsible for ICT coordination. While the architecture definition process provides good input for necessary changes to the governing entities, it would be obsolete to describe those operations in the architecture methodology.

The key concepts of the ZWoGA are:

- **Architecture domain** - a domain that at a high level encapsulates a set of concerns and issues. The domains are used as the first-level decomposition elements for the ZWoGA. These are architecture vision, integrated public service architecture, application architecture, technology architecture, data architecture, security architecture and governance architecture.
- **Artefacts** - are the architecture deliverables from each architecture domain that present an outcome of architecture work. This could be any bounded results such as a "statement" (as in the goal of architecture vision), a diagram, a table, or a list. The artefacts describe the architecture.
- **Building Block** - logical functional element defined as a result of the architecture work that is implemented as techno-organisational solutions (anything from "methodology" to "infrastructure solution"). Each building block must be assigned an owner who is responsible for the implementation and operation of the building block.

An overview of architecture domains is provided in the diagram Figure 5 Whole of Government Architecture definition methodology.

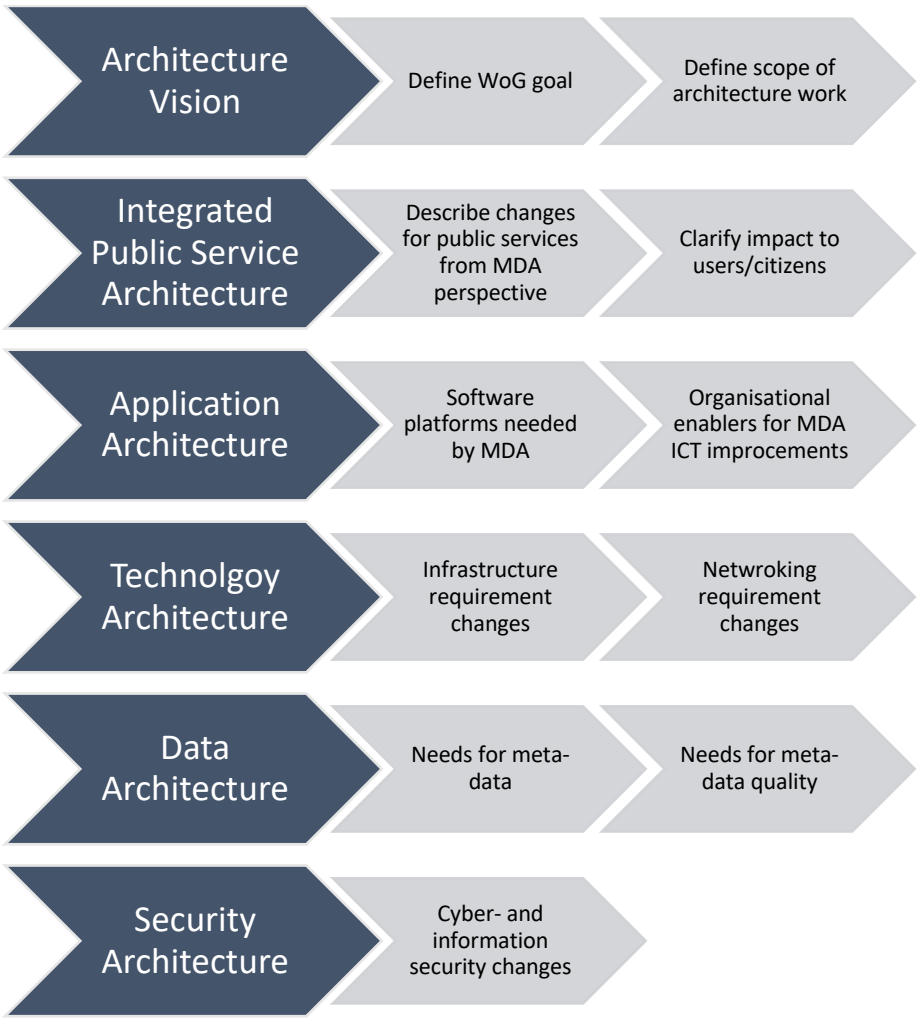


Figure 5 Whole-of-Government Architecture definition methodology.

3.1 Architecture Descriptions

The current methodology suggests combining architectural descriptions into roughly domain-based batches. This is relevant as some of the outputs are needed only for the core team responsible for orchestrating and guiding the architecture development work while other results need to be shared and populated with a wider set of stakeholders. The following table provides an overview of aggregate documents combining the results of the first architecture development iteration.

The target audience uses architecture organisations defined in the Governance Architecture - for clarification see the relevant document.

Table 4 Architecture Descriptions Overview

Index[1]	Output	Target audience
D3-2	EA Approach and Framework (current document)	For e-Government Technology Agency and Advisory Body for defining process for next architecture development iteration.
D3-3	Repository	For e-Government Technology Agency (expected owner and maintainer of repository) for managing requirements and plans for tools that support architecture development and implementation.
D4-1	Architecture Vision	All stakeholders and other related parties. For aligning general understanding of current architecture vision.
D4-2	Integrated Public Service Architecture	Respective architecture domain owner and selected working group (subset of advisory body) who is responsible for further development of the domain architecture and implementing defined building blocks.
D4-3	Application Architecture	Respective architecture domain owner and selected working group (subset of advisory body) who is responsible for further development of the domain architecture and implementing defined building blocks.
D4-4	Technology Architecture	Respective architecture domain owner and selected working group (subset of advisory body) who is responsible for further development of the domain architecture and implementing defined building blocks.
D4-5	Security Architecture	Respective architecture domain owner and selected working group (subset of advisory body) who is responsible for further development of the domain architecture and implementing defined building blocks.
D5-1	Governance Architecture	Advisory body and Government Chief Information Officer Council. Stating relationships for cooperation.

[1] Reference number that is relevant in the context of consultancy project An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe"

Index[1]	Output	Target audience
D5-2	Change Management Strategy	Advisory body and Government Chief Information Office Council. Handbook for engaging stakeholders for Architecture Development and Implementation.
D5-3	Roadmap	All stakeholders and other related parties. For aligning general understanding of current agreed work items and schedule.

3.2 Architecture Vision and Governance

3.2.1 Purpose

The Architecture Vision as a domain of architecture work is to establish a solid foundation for architecture development iteration. With that, it will engage stakeholders in the architecture development work, facilitate their involvement and establish a joint vision for the expected result and change in Zimbabwe.

The Architecture Vision phase accommodates architecture development initiation and facilitation work. Therefore, the phase could be seen as an umbrella over other phases and is concluded with a (not directly part of architecture development work) scheduling phase where a relevant roadmap is created. See Figure 6 and Figure 3 for visual representation.

Also, within the architecture vision domain, the Governance of architecture is handled not strictly from the architecture work scope (creating a target architecture and path to reach it) but also from the architecture implementation and plan execution perspective.

This means that the Governance structure is more focused on change implementation and management and the structure of governance should be reviewed when the next iterations of architecture are started - different goals might need different governance methods and models.

As the content for future architecture is something relevant for a wider set of audiences and governance aspects only specifically relevant to key stakeholders and working groups then it is advisable to keep the architecture content and governance models in separate documents (see Table 4 items D4-1 and D5-1).

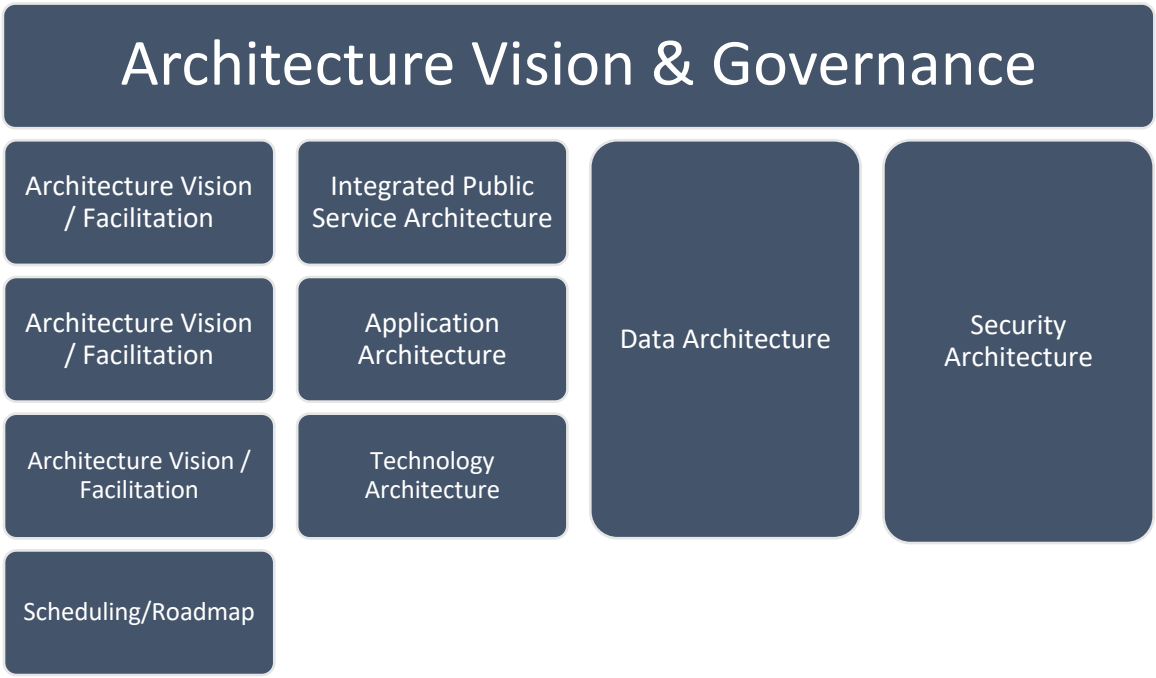


Figure 6 Generic plan of phases.

3.2.2 Participants

All stakeholders. If the motivation for architecture work is very strongly tilted to some specific direction a selection from all possible stakeholders can be engaged.

3.2.3 Steps

1. Engage stakeholders - define specific persons who shall be engaged for the duration of architecture development work and agree on potential contribution time expected for stakeholders.
2. Collect and review concerns from stakeholders. If the architecture design work was triggered by a specific requirement or change in the public sector or society make sure that this aspect comes out as a concern that will be addressed during this phase.
3. Identify opportunities and drivers for architecture.
4. Agree on a goal/vision for guiding architecture development work. The vision must be defined well enough so that all involved stakeholders would be ready to subscribe to the goal.
5. Conduct a preliminary risk assessment. Identify risks with their probability and impact. Define mitigation measures for the most critical risks (high impact, high probability at least).
6. Revise, adjust and add Key Performance Indicators (KPI) and metrics to measure the success of architecture - the metrics must be inspired by the agreed goal/vision.

7. Review the architecture governance structure and make necessary changes so that governance would support the implementation of the goal/vision.
8. Facilitate launching architecture development in other architecture domains. Some of those should be done in parallel.

3.2.4 Artefacts

Following the same logic as described above in chapter Steps - the artefacts created during the vision phase should be built gradually:

- Identifying and engaging stakeholders.
- Phrasing out the concerns and problems - what needs to be fixed.
- Defining the goal (key change) of the architecture.
- Understanding the limitations and context for the change - risks, metrics and potentially other framing artefacts.

3.2.4.1 Stakeholders catalogue

- A table, that should be publicly available for all stakeholders during the architecture development work.
- The table should contain the following fields for each stakeholder: name of organisation, name of the person assigned to the architecture work (can be several), role of the person in the architecture development work (contributor, validator, to be informed, etc.), contact information.
- The architecture development work coordinator/facilitator must ensure that the catalogue stays actual.
- During the initial gathering of contact information from stakeholders, it is also reasonable to collect information about existing skills and arrange training if it is relevant.

3.2.4.2 Catalogue of Concerns

- A list of high-level problems and issues that define the need for an improved architecture. The problems (the most important ones) must be addressed by the Architecture Goal Artefact.
- The Catalogue of concerns must contain for each concern the following attributes:

- Short name for the concern (label),
- description of the concern - why and what kind of issues it might cause,
- Importance of the concern - classifier to distinguish if the concern is **addressed** by current architecture work, will be **impacted** by current architecture work or left to be handled in the **future** if relevant.

3.2.4.3 Architecture Goal

- A descriptive document or part of an architecture vision description (it should also be considered if it is reasonable to expose as a presentation) composed of three main elements:
    - the architecture vision/goal statement(s) - short phrasing of the vision.
    - goal/vision description to expose the meaning of vocabulary used in the vision statement and
    - provide clarification or back-story for the vision statement.

3.2.4.4 Risk Catalogue

- A table of identified risks.
- Each risk should be described using the following elements:
    - Label or short description of the risk.
    - Description of risk.
    - Probability of risk on the relative scale: low, medium, high.
    - Impact of risk on the relative scale: low, medium high.
    - Description of mitigation - it is sufficient to describe mitigative measures only for risks where probability and impact are at least medium level.
    - The organisation that is responsible for mitigative actions.

3.2.4.5 Catalogue of opportunities and drivers

- A list of existing capabilities (both technical, organisational and social) that would be beneficial for architecture development.
- Each opportunity should be described with the following elements:
    - short name of the opportunity (label),
    - description of the opportunity,
    - main contact for getting additional information or using the opportunity (can be a reference to the stakeholder's catalogue).

3.2.4.6 KPI and metrics

- Catalogue of key performance indicators (KPI) for the architecture work.
- KPIs should be defined using Specific, Measurable, Achievable, Realistic, and Timely (SMART) principles.
- For each KPI a realistic method for measuring must be provided. KPIs without the potential to be measured should be disregarded.
- It is recommended to be conservative when removing or changing KPIs - having long-term KPIs helps to expose long-term changes.
- If needed additional KPIs can be introduced, but the total number of KPIs should be rather smaller to avoid spending too many resources on measuring.

- In the catalogue, each KPI should be described with the following elements:
    - KPI label - short descriptive label,
    - description of the measuring approach and techniques,
    - Initial value,
    - target value (for target date defined in architecture vision artefact.

3.2.4.7 Governance model

- Diagram resenting entities related to the governance of the architecture
- The diagram should include both - executive entities or roles and influencing entities that support the change management process.
- The diagram should also present the chain of command and/or influence.
- The architecture is not dictating if specific roles should be created as new positions - this is for decisions in each respective MDA where a new role is defined.

3.2.4.8 Roles and Skills

- Table consolidating overview of expected skills for key roles in the governance model.
- The table must contain the role, affiliation (which organisation or type of organisation the roles belong to), and key skills expected from the person fulfilling the role. Both professional and soft skills should be considered.

3.2.4.9 Governance and communication matrix

- A table/matrix defining communication channels and tools for each governance-related unit.
- The matrix should contain fields to describe:
    - The entity from the Governance model.
    - Purpose of communication.
    - Potential tools of communication.
    - Main target group(s).

3.3 Integrated Public Service Architecture

3.3.1 Purpose

Describe using architectural terms how stakeholders cooperate and collaborate when providing public services. The domain core is to address MDA cooperation in delivering public services using a cooperative approach - this defines integrated public service.

3.3.2 Stakeholders

MDAs that provide public services. From the entities, the roles responsible for the operations and design of public services must be assigned to this phase.

3.3.3 Steps

1. Refine the integrated public service conceptual model
    a. Using the existing model from the previous iteration identify where cooperation issues exist and what aspect of cooperation between MDAs/stakeholders needs improvement.
    b. If needed enhance the model to refine conceptual details of the problem area.
    c. Using the model identifies what concepts need refinement - these address other artefacts in this domain or provide input for changes in other architecture domains.
2. Revise and update what methodologies need to be added or enhanced to resolve problems and challenges with IPS development and implementation.
3. Revise and update what tools need to be added or enhanced to resolve problems and challenges with IPS development and implementation.
4. Revise and update what training (organised skill and capacity building activities) needs to be added or enhanced to resolve problems and challenges with IPS development and implementation.

3.3.4 Artefacts

3.3.4.1 Integrated Public Service Conceptual Model

Presents relevant concepts in the domain. It is critical to keep the level of details low and only refine relevant elements to be addressed in the current architecture iteration.

3.3.4.2 List of methodologies

A list of methodologies for IPS development and management. The list contains the following columns:

- the name of the methodology,
- description of what the methodology must deliver,
- target iteration of architecture - as some IPC challenges might require

3.3.4.3 List of tools for IPS development and management.

Table consolidating overview of necessary collections of tools for IPS architecture development and operation.

The table should be composed of at least the following columns:

- Name of toolset
- Description - key capabilities that the toolset must provide.
- Target iteration - reference in architecture cycles (or years) when the skill will be needed in the GoZ.

3.3.4.4 List of trainings for IP development and management.

Table to gather an overview of necessary training courses where continuous ability to raise capacity is needed. The table should contain at least the following columns:

- Training course name referring to the key skill.
- Description - brief description of most important course aspects and deliverables.
- Target iteration - reference in architecture cycles (or years) when the skill will be needed in the GoZ.

3.4 Application Architecture

3.4.1 Purpose

An Application Architecture describes the patterns and techniques used to design and build an application. The architecture gives a roadmap and best practices to follow when building an application, to end up with a well-structured app.

Therefore, it is essential to:

- identify and describe common requirements from MDAs to be able to provide public services as foreseen by integrated public service, and
- define the functional scope of platforms to address those concerns.

The Application Architecture will address the needs of MDA applications (synonym for information system), but the key deliverable of application architecture is an overview of the platform for the whole of government use. Although a platform is also an application these should be separated. A platform is a techno-organisational solution that helps MDAs implement and operate their information systems in the context of providing integrated public services.

3.4.2 Stakeholders

- Existing or potential e-Governance Platform Owners.
- Chief Development Officers, Chief Architects (or similar, responsible for ICT-related development plans) from participating MDAs.

3.4.3 Steps

1. Identify common needs of public service providers who have or are about to create an information system for their public service provision. The catalogue of concerns, architecture goals and integrated public service conceptual model should be used as input. It is important to identify needs that are not public service specific – rather the needs that are or can be relevant for other public services and public service providers must be focused.
2. Prioritization of most urgent needs among the stakeholders.
3. Revise the platform portfolio to identify if some identified need should be addressed by an already existing platform or if the need should be addressed by strictly organisational and/or legal measures (and leave it out of scope for application architecture work).
4. Add missing platform to platform portfolio and identify candidate owner.
5. Parallel to the previous step draft or update the Application-Platform interaction model to expose how the platforms are expected to empower MDAs and their information systems and react to the needs defined in the first step. The model should be sketched several times to reach an agreed common approach by the stakeholders involved in the current architecture work iteration.
6. Parallel to the previous step describe interfaces.

3.4.4 Artefacts

Application architecture artefacts are descriptions of application components, interfaces, and interactions, often represented through diagrams.

The following artefacts should be created during the process.

3.4.4.1 Common functional requirements

A model that is built on top of the Integrated Public Service Conceptual Model and that exposes the common needs of key stakeholders. This can be described as a listing or as a diagram exposing the source of a need.

3.4.4.2 Platform portfolio

List of existing or planned platforms (**NB!** Not applications of MDAs for public service-specific functionalities). The portfolio can be presented as a table of following content:

- Name of the application/platform.
- Key functional requirements.
- The principal owner of the platform (organisation and unit level precision expected).
- Architectural choices and principles for the platform.
- Candidate solution(s) - if any recommendations or suggestions are relevant.

3.4.4.3 Interface Catalogue

Describe high-level interfaces of platforms. The content of the Catalogue will define the principal properties of how applications are interfaced with platforms and platforms among themselves. The Catalogue must be described only for the platforms identified for adoption and immediate implementation. Together with the platform portfolio, the interface catalogue is the key input for implementing/procuring the changes to platforms. The Catalogue of interfaces must be described using the following characteristics:

- A platform that provides the interface.
- Interface name.
- Key functionality.
- Design principles for the interface.

3.4.4.4 Application-Platform Interaction Model

Considering a generic integrated public service scenario demonstrates the cooperation and flow of public service exposing how the platforms are empowering the information systems of MDAs for the provision of integrated public services. The model should expose the platforms, usage of their interfaces and order of interaction with information systems (MDA applications).

3.5 Technology Architecture

3.5.1 Purpose

Expose the low-level dependencies and baseline services that are needed to implement MDA information systems (instructed and motivated by IPS architecture) and building blocks defined by application architecture. The Technology Architecture discipline must ensure that the SLA of infrastructure and baseline services and expectations from MDAs are aligned.

3.5.2 Stakeholders

Technology Architecture should be developed by engaging CTOs from existing platforms and key MDAs (selected at the beginning of architecture initiation work). According to interest and motivation experts of infrastructure and networking could be included in the core circle of stakeholders should be the following:

- Existing or potential e-Governance platform owners (Application Architecture).
- CTOs and Chief Architects of entities providing infrastructure, networking and commodity IT services.
- Chief Technology Officers (CTOs) representing MDA's current and future expectations on technology architecture.

3.5.3 Steps

1. Map long-term technology requirements
    a. Through stakeholder engagement - results of Architecture vision, IPS architecture and application architecture work - collect long-term technical capability development directions (rather than technology requirements).
    b. Information about ICT baseline tools (collaboration, office coworking, general administrative needs) should be collected to identify potential common interests towards baseline IT. For existing baseline tools, the satisfaction with those tools should be identified and reasons for unsatisfaction exposed.
    c. Consider also expectations by wider society (network and infrastructure availability for end-users).
2. Emerging technologies must be kept on the radar and assessed for relevance to the architectural goal and the long-term viability and sustainability. For reasonable options, the technology services matrix should be revised and analysed (mostly from the sustainability aspect) if adopting an emerging technology would make sense to reach the architecture goal.
3. Identified long-term requirements and trends must be mapped against current capabilities to identify critical deficiencies. The challenges discovered must be compared to the list of existing policies (as the instrument of defining the cooperation model with other sectors). The existing policies might be rewritten, or some new policy composed.
4. The technology services (building blocks of technology architecture) matrix must be revised to add new ones or dismiss those that are not relevant.
    a. For added (or significantly changed) services the ownership must be set and the principal plan of establishing the service defined.
    b. For deprecated and removed technology services the phase-out plan must be sketched as part of the building block description.

3.5.4 Artefacts

The following artefacts will be delivered because of the Technology Architecture development.

3.5.4.1 Technology Policies Catalogue

The Catalogue should list topics that have or need a policy. These can be already adopted and valid policies but also could identify policies that are to be developed during architecture implementation. For each policy, the catalogue should contain the following information:

- **Topic** - the topic on which a policy must be defined and agreed upon among stakeholders.
- **Key Problem** - brief description of the problem that the policy gives clarity and instructions.
- **Owner** - organisation and position (if obvious also the name of the person) of who is responsible for running the policy development and monitors the policy implementation and fulfilment.
- **Adoption date** - expected deadline for approving and adopting the policy. This should be seen as a target date for policies to be written or an actual adoption date for existing policies.
- **Status** - identify the status of the policy at the time of architecture work. This could be one of the following:
    - **Draft** - the policy is being drafted.
    - **Adopted** - the policy is finished and approved by the relevant process.
    - **Deprecated** - policy has become irrelevant and is not valid anymore.
- **URL** - where the policy (regardless of the status) can be found.

3.5.4.2 Technology Services Matrix

Overview of services that are expected from the technology architecture layer. Each service constitutes a technology building block and should be in the matrix described in a few critical elements:

- **Service Name** - the name of the services required by the MDAs and application architecture platforms.
- **Owner of the services** - organisation and department/unit name responsible for delivering the service and defining its SLA.
- **Description** - brief description of the service. More thorough exposure of each service (with requirements for its construction and operation) should be described separately.

3.5.4.3 Emerging Technologies Matrix

Overview of emerging technologies and key results of their assessment status. The catalogue should contain the following information:

- **Name of the emerging technology**
- **Date of last assessment** - date of the assessment.
- **Key benefits** - features that make the technology promising and desirable from the perspective of Zimbabwe.
- **Key threats** - aspects and risks that should be considered as potentially dangerous. This should provide the key arguments for why an emerging technology should not be adopted.

- **Position** - the result of the analysis should propose a recommended status for the specific emerging technology. The status should be one of the following:
    - **Adopt** - the emerging technology is favourable, accepted in the local ICT community, and has clear benefits and a sustainable perspective. It should be adopted, and it should be tailored into ZWoGA.
    - **Monitor** - the emerging technology is promising in its delivery value, but other aspects are not mature enough for adoption. The evaluation should be repeated in the next architecture iteration.
    - **Ignore** - the emerging technology has significant sustainability issues or threats to be of interest. To avoid repeating re-analysing ignored emerging technologies it is recommended to keep in the artefact information of up to 5 years old assessments.

3.6 Data Architecture

3.6.1 Purpose

Describe needs related to information for managing work and content in other domains - meta-data needs. Make agreements about the meta-data gathering process.

3.6.2 Stakeholders

Representatives from all Stakeholders must be involved as the needs for information might be various.

3.6.3 Steps

- Gather meta-data requirements from stakeholders.
- Revise catalogues and work out necessary changes - additional, removals or changes to meta-data catalogues.
- Revise the quality aspects of meta-data and find owners for quality concerns.
- Draft meta-data harvesting/collection process.

3.6.4 Artefacts

Data Architecture artefacts are data models, data flow diagrams, and data dictionaries that define how data is stored, processed, and accessed.

3.6.4.1 Quality Constraints

To consolidate requirements and expectations on the quality of meta-data.

The constraints must be listed as a table with the following columns:

- **Quality constraint** - aspect of meta-data that needs attention.

- **Improvement measures** - mechanisms to ensure that the quality of meta-data is managed.

3.6.4.2 Catalogue of Organisations

To understand all the stakeholders. The following minimal structure is expected to describe the catalogue content:

- **Meta-data field** - an identifier of a meta-data field.
- **Description** - semantical meaning of the field.
- **Use-case or purpose** - why the information is relevant and for whom.

3.6.4.3 Catalogue of Public Services

To understand - for governance and integration purposes - what services (in the future "digital services") are there in the GoZ.

- **Meta-data field** - an identifier of a meta-data field.
- **Description** - semantical meaning of the field.
- **Use-case or purpose** - why the information is relevant and for whom.

3.6.4.4 Catalogue of Information Systems

To contain and aggregate information about information systems in the public sector. The information about the catalogue should be documented by:

- **Meta-data field** - an identifier of a meta-data field.
- **Description** - semantical meaning of the field.
- **Use-case or purpose** - why the information is relevant and for whom.

3.7 Security Architecture

A Security Architecture is a set of models, methods, and security principles that align with objectives of technology, data, application and integrated public services, keeping your GoZ and MDA systems and services safe from cyber threats. Through Security Architecture, business requirements are translated to executable security requirements.

3.7.1 Purpose

The main purpose of security architecture as an architecture domain is to reduce the risk of sensitive data breaches and/or manipulation through integrated public services and MDA organizations and systems from threats while digitalisation becomes more dominant. Embedding security into business operations is a core idea for Security Architecture.

3.7.2 Stakeholders

- Government Chief Information Security Officer (GCISO, to be appointed),
- CISOs or Security Architects from MDAs (to be appointed),
- Members of the Cybersecurity Committee (to be established), and
- Representatives of NCIRT (to be established).

3.7.3 Steps

As the current Cybersecurity organisation in Zimbabwe is being implemented then the steps and artifacts of the first architecture development integrations are significantly different from expected future security architecture development iterations.

1. Analyse concerns and risks, and find aspects where the security approach needs adjustment and refinement.
2. Revise that metamodel for Information System Management System (ISMS) - make changes so that it would provide necessary information for dealing with concerns and risks identified in the first step.
3. Review non-functional requirements from the perspective of concerns and risks. Add or remove items. In later architecture development iterations, the following concepts can be introduced for NFR:
    a. non-functional-requirement owner - who is interested in a specific non-functional requirement,
    b. non-functional-requirement validation mechanism.
4. Identify new stakeholders whose infrastructure is critical and review critical infrastructure protection methods.
5. Revise working practices related to incident discovery and response to match changed situations.
6. Review security-related policies - remove obsolete ones and define a plan to create new ones.

3.7.4 Artefacts

Security Architecture artefacts are described below.

3.7.4.1 Policies

Security-related Policies are described as a table following the same structure as described for Technology Policies Catalogue artefact in chapter 3.5.4.1.

3.7.4.2 Non-functional Requirements

Non-functional Requirements are to be described as a table composed of the following columns:

- **Type or Category** - requirements should be aggregated into groups of similar requirements for easier reading.
- **Reference Number** - a two-position number where the first number identifies the category, and the second number identifies a specific requirement.
- **Requirement** - description of the requirement.
- **Owner** - person or role/position and organisation of who is interested in such requirement.
- Each requirement could be enhanced to validation mechanisms (how to check if the requirement is met or not) and alternative solutions.

3.7.4.2.1 Critical Information Infrastructure Service Providers

List of Critical Information Infrastructure and vital service providers for whom additional requirements and assistance for security implementation should be applied.

For each service provider in the list, the following information elements must be provided:

- Name of the organisation and contact details,
- Service that has a critical or vital nature,
- Service category (or type of service) to aggregate similar service providers,
- MDA who is responsible for the specific service.

4 Changes for Next Iterations

Upon initiating a new architecture definition iteration, it is relevant to address some key aspects:

- Conduct a self-assessment to identify the aspects where shortages are most significant. This is from both the content and methodology perspective. Where necessary adjust the methodology.
- Reserve resources (time to work, finances etc.) for the architecture definition work. These resources are not for architecture implementation work but for architecture definition that results in an updated (or new) roadmap.
- Assign a core team that is responsible for completing the architecture definition iteration. The team should be composed of at least the following roles:
    - **Donor** - the role or person most interested in updating the architecture. Responsible for ensuring that necessary resources and stakeholders are engaged.
    - **The Project Manager** - keeping track that the architecture development iteration would reach a tangible result within allocated resources.
    - **Chief Architects** - role responsible for keeping the work content on track.
- Plan the architecture development iteration to overlap with a budget planning cycle to be able to address also budgeting aspects within the roadmap update.

5 Annexe 1: Results of the practical workshop

In January 2024, eGA experts facilitated an interactive 3-day workshop in Zimbabwe, bringing together key stakeholders from the public sector. The primary objective of the workshop was to delve into Zimbabwe's current digital landscape and Enterprise Architecture, exploring existing strategies, plans, and perceived challenges. Through collaborative discussions and knowledge sharing, participants gained a comprehensive understanding of the country's digital development readiness and identified avenues for modelling the Zimbabwean whole of government (enterprise) architecture (ZWoGA).

The workshop addressed critical pillars of Enterprise Architecture through eight exercises, starting with identifying the main goal of the ZWoGA, addressing user groups and their needs, identifying priority baseline principles and domains of the ZWoGA, and highlighting different approaches to ensure effective communication and coordination to develop and maintain the whole of EA.

5.1 Exercise 1

The initial exercise tasked participants with **defining the overarching goal for the ZWoGA**. Collaboratively, representatives from OPC, MOICTPCS, and various MDAs concurred that the primary goal would be to "**Establish a strategic framework facilitating the alignment and integration of government ICT infrastructure and systems**."

The goal is to be revised in the upcoming stages of the project.

5.2 Exercise 2

In the second exercise, participants were tasked with **identifying the foundational principles for developing the ZWoGA**. From a list of 30 predefined principles, attendees collectively identified five critical baseline principles. These principles were selected based on their significance in guiding the establishment and implementation of the ZWoGA framework, and the selection was as follows.

1. **User-Centric**. Service delivery follows a user-centric approach.
2. **Security**. Data privacy, authenticity, and integrity are guaranteed.
3. **Reuse**. Users must provide the same data to the government only once.
4. **Secure**. Development processes and standards enforce quality and security.
5. **Robust**. Solutions are easily scalable for high availability and reliability.

5.3 Exercise 3

The third exercise aimed to pinpoint the **primary user groups of the ZWoGA**. Participants engaged in selecting five key roles from a predefined list of roles, including:

- Chief Technology Officer (CTO),
- Enterprise Architect,
- Architecture Sponsors,
- Researchers, Educators and
- System Analyst.

5.4 Exercise 4

Following the selection of user groups, in exercise four, participants were tasked with defining the specific **requirements and needs of each user group.** The needs of each user group were identified as presented in the following table:

Chief Technology Officer (CTO)	Enterprise Architect	Architecture Sponsors	Researchers and Educators	System Analyst
Leading role	Scalability	Cost effective structure (budget estimates)	Mentorship and guidance	IT landscape overview
Interoperability requirements	Hardware and software specifications	Risk register	Accessibility and availability of information	System interoperability and integration
Methodologies	Accessibility and availability (bandwidth, speed)	Change management plan	Training plan	Data architecture
Standards	Resilience of systems (multiple accessibility)	Strategic alignment	Standards and best practices	Technology architecture
Technology Standards	Business process assessment	Business and technology goals and objectives	Frameworks and models	Application architecture
Acceptable Technologies and Infrastructure	Organizational skills/capacity	Standards	Case studies and success stories	Security architecture

Chief Technology Officer (CTO)	Enterprise Architect	Architecture Sponsors	Researchers and Educators	System Analyst
Security	Security operations in IT	Integration and interoperability plan	Information on data governance	Business processes and workflows
Governance	Methodologies	Communication plan and reports	Governance and change management	Technology guidelines and standards, documentation and communication
Strategic plans	Interoperability	Theory of change	Security and privacy considerations	IT governance and policies, procedures and structures
Funding		Value for money (benefits)	Innovation and improvement	Solution design
Innovations		Architectural vision and mission		Change management
		Stakeholder management		Risk assessment
		Risk management		
		Implementation roadmap		
		Benefits and value proposition		

5.5 Exercise 5

In the fifth exercise, the focus was on **identifying the primary enterprise architecture domains**, which serve as descriptions or representations of the various layers within the enterprise architecture framework. Through collaborative efforts, stakeholders collectively identified five main domains: Business architecture, Data architecture, Application architecture, Technology architecture, and Governance architecture.

5.6 Exercise 6

During exercise 6 of the workshop, participants were tasked with **defining the effective communication** tools essential for ensuring the appropriate development of enterprise architecture. The main channels identified as suitable by the attendees included Inter-Ministerial Meetings facilitated by liaison officers, and dedicated individuals responsible for communication and coordination between Ministries, Departments, and Agencies (MDAs). Additionally, Working Groups, Digital Communication Platforms such as Slack, Microsoft Teams, Emails, WhatsApp, and Viber groups, as well as Collaborative Decision-Making Bodies comprising committees with high-level representatives from each MDA were recognized. Cross-training programs and top-down communication were also highlighted as valuable communication mechanisms. These channels collectively contribute to fostering effective communication and collaboration necessary for the successful implementation of the ZWoGA.

Furthermore, participants voiced their concerns regarding **communication and coordination challenges**, highlighting several issues currently faced by Zimbabwe. These include constraints such as limited budgets for licenses, hardware, and digital platforms, as well as infrastructural limitations and connectivity deficiencies. Bureaucratic processes, short notices, and poor planning were also identified as impediments, along with slow dissemination of information and a lack of message clarity. Additionally, resistance to change and the difficulty of gathering individuals in one location due to budget constraints were noted. These challenges underscore the complexities involved in effective communication and coordination within the Zimbabwean context, calling for innovative solutions and collaborative efforts to address them comprehensively.

5.7 Exercise 7

In the seventh exercise, participants were assigned the task of **identifying the main five organizations**, in addition to the OPC and MOICTPCS, that should be consistently engaged **as key stakeholders** throughout the entire process of developing and implementing a ZWoGA. Attendees highlighted critical stakeholders as:

- the Ministry of Finance, Economic Development and Investment Promotion,
- the Ministry of Home Affairs and Cultural Heritage (MOHA),
- the Ministry of Higher and Tertiary Education, Innovation, Science, and Technology Development (MHTESD),
- the Public Service Commission (PSC), and
- TelOne.

These organizations play integral roles in various aspects of government operations and policymaking, making their continuous engagement essential for the success of the ZWoGA initiative.

5.8 Exercise 8

In the concluding exercise, participants were prompted to share their perspectives on the **factors driving stakeholders to actively participate** in the development, implementation, and maintenance phases of the ZWoGA. Representatives from various MDAs emphasized capacity building and knowledge exchange as significant elements influencing their engagement. Recognizing the importance of continuous learning and information sharing, stakeholders highlighted these aspects as key motivators for their involvement.

The analysis of data gathered from the eight exercises has provided invaluable insights into the modelling of the ZWoGA. Through collaborative efforts and thoughtful deliberations, participants have identified key components such as the overarching goals, baseline principles, user groups, communication tools, organizational stakeholders, and motivating factors for engagement. By delineating enterprise architecture domains and addressing communication and coordination challenges, stakeholders have laid a solid foundation for the development, implementation, and maintenance of ZWoGA. Moving forward, the findings and recommendations derived from these exercises will serve as a roadmap for enhancing digital development, fostering interoperability, and promoting efficient governance across government entities. The active engagement and commitment demonstrated by participants underscore the importance of continued collaboration and collective action in shaping the future of enterprise architecture within the Zimbabwean context.

D3-2 Enterprise Architecture Repository

The Consultancy Services for the Government of Zimbabwe Enterprise Architecture Modelling Exercise

Table of Contents

Abbreviations and Acronyms

Acronyms	Descripton
EA	Enterprise Architecture
eGA	e-Governance Academy, Estonia
IT, ICTs	Information and Communication Technology/-ies
MDAs	Ministries, Departments and Agencies, Zimbabwe
MICTPCS	Ministry of Information Communication Technology, Postal and Courier Services, Zimbabwe.
OPC	Office of the President and Cabinet, Zimbabwe
ZWoGA	Zimbabwe Whole of Government Architecture

1 Introduction

The Architecture Repository is a critical component of architecture development. It is a managed repository that stores all architectural information, models, and artefacts that are created during the architecture development work.

Repository as a tool facilitates collaboration between a diverse group of stakeholders across the organization, from business strategy to IT.

The current document makes recommendations for tooling. The tools themselves (licenses, training, setup and customization) are not part of the deliverables and it is expected that the project team from OPC shall take care of setting the selected tool up and populate with initial project results.

The objective of the current study is to give options for the Zimbabwe Office of the President and Cabinet (OPC), and the Ministry of ICT, Postal and Courier Services (MICTPCS) for choices of appropriate tools to collect, keep and update documentation and process of Zimbabwe Whole-of-Government Architecture (ZWoGA) development available and co-operative.

The document provides:

- more context on the situation in Zimbabwe, ideas of base, transition and target repositories and expectations about licensing, prices (introduction, paragraphs 1.1 – 1.5),
- general requirements when choosing a tool (paragraph 2),
- lists best practices in use around the world (paragraph 3).
- Finally, it proposes the structure of the transition repository (minimum viable repository) to be prepared by eGA and to be used during the next iterations of ZWoGA by different stakeholders (paragraph 4).

1.1 Context of Zimbabwe

During practical workshops conducted in Zimbabwe in January 2024, participants were tasked with **defining the effective communication** tools essential for ensuring the appropriate development of enterprise architecture.

The main channels identified as suitable by the attendees included the Inter-Ministerial Meetings facilitated by liaison officers, and dedicated individuals responsible for communication and coordination between Ministries, Departments and Agencies (MDAs).

Additionally:

- Working Groups, Digital Communication Platforms such as
    - Slack,

        - Microsoft Teams,
        - Email,
        - WhatsApp, and
        - Viber groups, as well as
        - Collaborative Decision-Making Bodies comprising committees with high-level representatives from each MDA were recognized.
    - Cross-training programs and
    - Top-down communication.

These channels collectively contribute to fostering effective communication and collaboration necessary for the successful implementation of the Zimbabwe Whole-of-Government Architecture (ZWoGA).

Furthermore, participants voiced their concerns regarding **communication and coordination challenges**, highlighting several issues currently faced by Zimbabwe. These include constraints such as limited budgets for licenses, hardware, and digital platforms, as well as infrastructural limitations and connectivity deficiencies. Bureaucratic processes, short notices, and poor planning were also identified as impediments, along with slow dissemination of information and a lack of message clarity.

These challenges underscore the complexities involved in effective communication and coordination within the Zimbabwean context, calling for innovative solutions and collaborative efforts to address them comprehensively.

1.2 Baseline

Initial project documentation and contract materials, catalogue templates, materials from workshops, etc., are made available using tools that are agreed upon during the initial project. The document uses MS Office format, illustrations and sketches are made/ created with Mural[2]. See the approach and framework deliverable description for further details.

1.3 Target Repository

The Target Repository should be used for the governance and long-term maintenance of the Enterprise Architecture for the Zimbabwe Whole-of-Government Architecture.

A repository is a long-term tool; it should survive several Architecture development and implementation iterations over many years.

[2] https://www.mural.co

As a potential extension when the Architectural content grows bigger, instead of one / central Repository, it could be even considered to develop two repositories:

- **Repository of Interoperability Architecture.** OPC and MICTPCS are coordination and supervision bodies, responsible for the development, implementation and management of ZWoGA enablers.
- **Repository of MDAs and Local Government solutions.** MDAs and Local Governments (provinces/districts) are responsible for creating their own business, data, applications, and technical architecture in line with the overall ZWoGA and following/using its enablers.

Note! Specific target repositories for MDAs and Local Government solutions are not part of the proposal and it is suggested that the project team of the Government of Zimbabwe shall take care of selecting and configuring the desire tool as feasible for them as well.

1.4 Transition Repository

Due to the limited resources of OPC / MICTPCS, it is expected that the Target Repository will not be created in the first iteration. Rather, the Base Repository from initial EA project tools should be moved to a technology platform selected in conjunction with the representatives of OPC and MICTPCS, ideally during the project.

The structure of the repository must be developed. The Repository structure must be suitable for the governance and long-term maintenance of the enterprise architecture.

Creating target repository(-ies) will be foreseen in the roadmap.

1.5 Licensing, Price

The maintainer of the repository is looking for solutions and platforms that have no direct cost and would be preferably hosted using infrastructure from Government of Zimbabwe. Although with good reasoning on-cloud services would be viable. The total cost of ownership (hosting, maintenance, etc.) will be borne by OPC general costs.

There are no specific constraints in terms of licensing.

2 Requirements

The following list presents requirements that are to be addressed when building a repository and filling it with content. The repository is to be improved over time and the requirements should be focused towards a continuously improving repository solution. The requirements should be revisited at the beginning of each architecture iteration and agreed on how the requirements are going to be met (or dismissed).

1. **Document Profiling and Metadata**

   1.1. The repository should allow users to assign relevant Metadata (such as document type, author, and creation date) to each document.
   1.2. Metadata helps in efficient search, categorization, and retrieval of documents.
   1.3. Documents have a common naming schema.

2. **Document Storage and Organization**

   2.1. The system must provide a secure repository for storing electronic documents.
   2.2. Documentation includes texts, illustrative graphics, schemas, introductory and teaching materials, videos, co-operative tools, and dashboards.
   2.3. Storage should support folder structures, tags, and other organizational methods to arrange documents logically.
   2.4. Documentation must be linkable. Avoid one big and common file.

3. **Version Control**

   3.1. The repository should maintain a history of document versions.
   3.2. Users should be able to track changes (who, when, what), revert to previous versions, and collaborate seamlessly.

4. **Access Control and Permissions**

   4.1. Define user roles (e.g., admin, editor, viewer) and their access rights.
   4.2. Ensure that only authorized personnel can create, modify, or delete documents.
   4.3. Specify the availability of commenting documents by readers.

5. **Search and Retrieval**

   5.1. Implement robust search functionality to locate documents based on keywords, metadata, or content.
   5.2. Quick retrieval is essential for productivity.

6. **Workflow Automation**

   6.1. Define workflows for document approval, review, and collaboration.
   6.2. Automate notifications and routing based on predefined rules.
   6.3. One or a few Chief Architects must create the initial structure of documentation.

6.4. Experts on different areas (area managers) are asked to fulfil the structure with content.
6.5. Schema of authoring the changes is not required. (A Schema)
6.6. Comments from readers must be reviewed and resolved by respective area managers.

7. Integration between Editors, other Documents, and Systems

7.1. Co-edit availability of documents is essential, it makes co-operation productive.

7.2. Documentation must be linkable. Avoid one big and common file.

8. Document Security

8.1. Protect sensitive information through access controls.
8.2. Version history / audit trails should track document activities.

9. Document Retention and Archiving

9.1. Specify Retention Policies (e.g., delete after a certain period).
9.2. Archive older documents for compliance and historical purposes.

3 Review of Tools

The following table provides an overview of tools mostly used in the toolset of architecture work at the time of the current project. It is relevant for the team that is managing the architecture work to monitor for available market and capabilities, and skills of contributors. Based on those aspects proper tooling should be revised at the beginning of each architecture work iteration. However, the time needed to migrate from one tool to another must be planned and the migration complexity must be balanced out with the potential benefit of new tools.

The list of tools exposed here is wide as the good selection depends on understanding the way stakeholders are ready to receive information and contribute. This must be identified by the team during the first iterations of architecture work.

Category	Tool	Description	Pricing
Collaboration	Revver	File organization and workflow management considering remote teamwork.	Custom
Collaboration	Hightail	Focus on large images and video files	Free plan available; paid plans start at $12/month
Collaboration	Git	Tool for storing digital artefacts and managing their lifecycle as versions. Good for technicians, hard to use for non-technicians.	Free
Collaboration	Box	Extendable cloud-based content management system with collaboration, security, analytics.	
Content Management	Alfresco	Secure Content Management solution for distributed teams	Custom
Content Management	FileHold	Content Management system with an anonymous access portal	Custom
Content Management	OpenKM	Document Management with support for integration to other applications	Free plan/custom quote
Site Builder	Microsoft Sharepoint	Good ability to set permissions on sensitive documents when working with team-mates in different locations. SharePoint's versioning	From $5/user/month

Category	Tool	Description	Pricing
		feature has the iterative nature of designs and processes.	
Site Builder	Wix	Cloud-based Web Development Services. It offers tools for creating HTML5 websites and mobile sites using online drag-and-drop editing. Able to integrate with major social media platforms.	
Site Builder	WordPress	Popular and highly customizable site building platform as a service (wordpress.com) or on-prem solutions (wordpress.org, GPLv2).	On-prem: free, Hosted: starting $48/year
Cloud Storage	Dropbox Business	File Storage, sharing and connectivity to other online applications and services.	Starts at €16/user/month (annual billing)
Cloud Storage	Google Drive & Docs	Well supported parallel work on online resources.	Free; paid plans start at $12/user/month (annual billing)
Cloud Storage	OnlyOffice	Document Management and editing with collaboration and good tracking on contributions.	Cloud: from $1/user/month (3-year plan) On-prem: start at $2,200.
Modelling	Gliffy	Diagramming via an HTML5 cloud-based app. supports UML, Venn, Flowchart and additional stencils.	
Modelling	Diagrams.net	Previously draw.io. Alternative to Gliffy.	
Modelling	MS Visio	Modelling tool from Microsoft Portfolio.	Custom
Modelling	Mural	Infinity wall sketching tool oriented for collaboration of remote teams and online meetings.	Free plans and annual professional licenses.
Modelling	Archi	Tool supporting ArchiMate modelling language from The Open Group. Enterprise Architecture	Free

Category	Tool	Description	Pricing
		focused. Good for architect but hard to grasp for others.	
Collaboration	Confluence	Atlassian Application built on Jira that allow to build sites. As software for on-prem or service.	Custom

4 Initial Tools for ZWoGA

As ZWoGA is something that has many stakeholders who must work and align their activities in the same information room, it is recommended to use server-based repositories.

The list presented below is compiled in cooperation with eGA and OPC representatives.

4.1 Minimum Viable Product

As the focus of ZWoGA is to encourage and thrive the cooperation between stakeholders, then it is not reasonable to bloat the cooperation with new tools. There is a very high risk that with introducing a toolset at an early stage, the stakeholder's focus and discussion falls into discussing the tools and not what the tools are used for.

As an initial minimal viable product for architecture repository, an OPC controlled file-sharing website is recommended.

While the file-sharing website helps to structure the way, stakeholders are reaching out for the materials, the deliverables and descriptions of ZWoGA ideas must be in an easily processable format.

4.2 Structure

The initial folder and file structure of the MVP Repository is suggested as follows.

- **root** folder presenting the strategic level.
  - **current-architecture** – link to the folder with the currently approved architecture description version (initially pointing at "v1.0 architecture").
  - **draft-architecture** – link to the folder to architecture that is currently being described (initially pointing at "v2.0 architecture").
  - **events** – folder for architecture development and implementation event-related materials (slides, recordings, ...). Content should be built as "folder per event". For example:
    - **20241007-v1-handover** – folder containing materials about the handover event from the 7th of October 2024.
    - ...
  - **v1.0 architecture** – folder containing the deliverables of one specific architecture folder and represents the project level of materials.

        - **0 background** – folder containing collected analysis and background describing documents (or links to external sources) that provide context to the architecture iteration.
        - **0 methodology** – folder containing methodology description that was used to create this version of the architecture. The folder should always contain also an architecture meta-model that is relevant for the current iteration.
        - **1 vision** – folder containing architecture vision documents and artefacts.
        - **2 integrated-public-service** – folders containing integrated public-service architecture documents, standards, examples, templates and artefacts.
        - **3 application architecture** – folder containing application architecture documents, standards, examples, templates and artefacts.
        - **4 technology architecture** – folder containing technology architecture documents, standards, examples, templates and artefacts.
        - **5 data architecture** – folder containing data architecture documents, standards, examples, templates and artefacts.
        - **6 security architecture** – folder containing security architecture documents, standards, examples, templates and artefacts.
        - **7 governance architecture** – folder containing governance architecture documents, standards, examples, templates and artefacts.
        - **8 implementation** – folder containing roadmap and other guiding documents and artefacts for the implementation including decisions, compliance and capability assessments and performance measures.
    - **v2.0 architecture** – placeholder folder for future architecture version. Follows the structure of "v1.0 architecture" unless the methodology suggests some changes.
    - **v3.0 ...** – etc.

4.3 Toolset

Documents – it is recommended to use the most prominent and well-adopted format and solution for creating documents. The recommendation is to use **MS Office** (Word, Excel, PowerPoint).

Diagrams and models – use the online sketching solution **Mural** (a mural board created under an OPC account), as this is easy to learn and enables collaborative sketching, voting, annotating, etc. on one board. Keep only the "editable" versions in Mural and export intermediate versions of diagrams and illustrations as PNG files to the repository file system and/or document as needed.

Metadata – it is suggested to keep document version history, i.e. version number, date, author and short description of changes manually within the document itself. It is suggested to avoid using metadata as part of document name. If needed, then older versions of any document might be temporarily held in subfolder 'old' or 'archive' or similar within structure.

D4-1 Architecture Vision

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Index of Figures

Index of Tables

1 Executive Summary

This document outlines the strategic framework for the Zimbabwean Whole of Government Architecture (ZWoGA), aimed at enhancing the efficiency, transparency, and accessibility of public services through integrated ICT infrastructure.

The development of the Whole-of-Government Enterprise Architecture for the Government of Zimbabwe is led by the Office of the President and Cabinet (OPC). In addition, the document identifies other crucial stakeholders such as various Ministries, Departments, and Agencies (MDAs), and addresses their concerns and objectives regarding the Enterprise Architecture.

Key challenges such as resistance to change, varying digital maturity levels, and legacy system integration are highlighted, along with strategies for overcoming them.

The document also presents a high-level target architecture emphasising principles like Data Privacy, User-Centric Service Delivery, and Scalability.

The ZWoGA aims to provide a unified approach to ICT development, fostering cooperation among MDAs and leveraging emerging technologies to improve public service delivery.

Metrics and KPIs are designed to measure progress, ensuring continuous improvement and alignment with strategic goals.

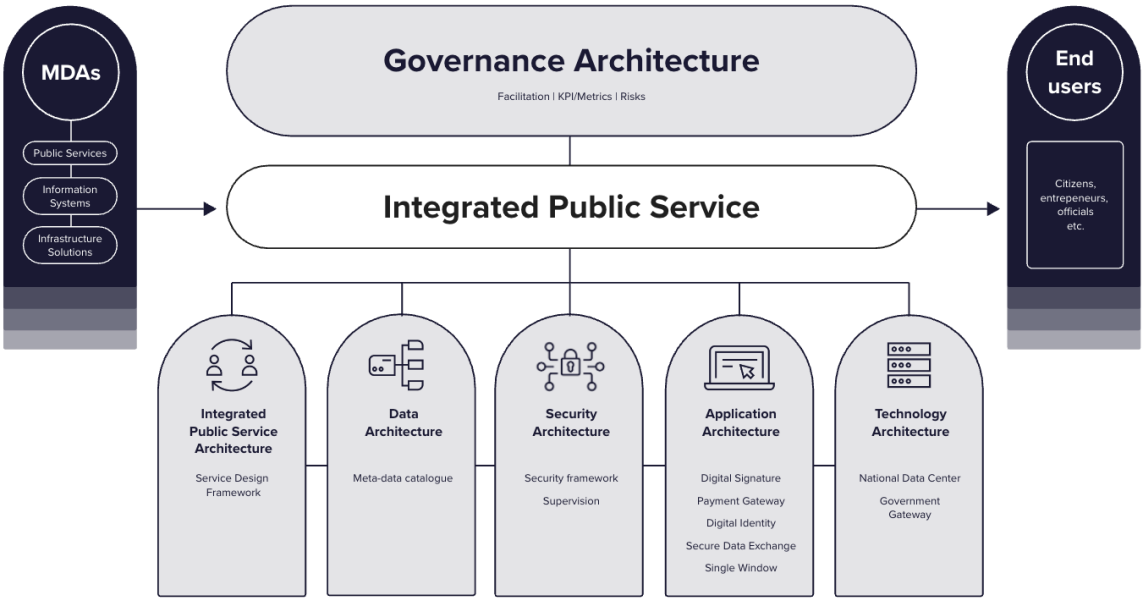


Figure 7 Zimbabwe Whole of Government Architecture

2 Purpose of the Document

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the "An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for enterprise architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to enterprise architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

This document serves as a vital reference for all other architecture domains within the Zimbabwean whole of government architecture (ZWoGA) by providing a unified framework. This document establishes the strategic direction, goal and guiding principles that inform the development and integration of various other architectural domains such as business, data, application, and technology architecture among others.

Chapters of this document are outlined as follows:

- Chapter 3 introduces the key stakeholders, including the Office of the President and Cabinet (OPC) and other important entities.
- Chapter 4 presents various artefacts and explains the necessity for the ZWoGA. It highlights the main concerns identified by MDAs, showcasing the Zimbabwean government's strengths as a driver of change and the opportunities for successful ZWoGA implementation. This chapter also outlines the agreed ZWoGA goal by MDAs and explains how the planned architecture will achieve set objectives and address key concerns. Additionally, it explores the identified risks and presents approaches to measure the success of implementation through various KPIs recognized by MDAs.
- Chapter 5 discusses the impact of digitalized integrated public services compared to the current system, where citizens are responsible for collecting necessary information to obtain public services.
- Chapter 6 presents the high-level target architecture, emphasizing the main principles agreed upon by MDAs to be integrated into the ZWoGA as the initial

phase. It also outlines the necessary policies to support the smooth operation of ZWoGA.

2.1 Methodology

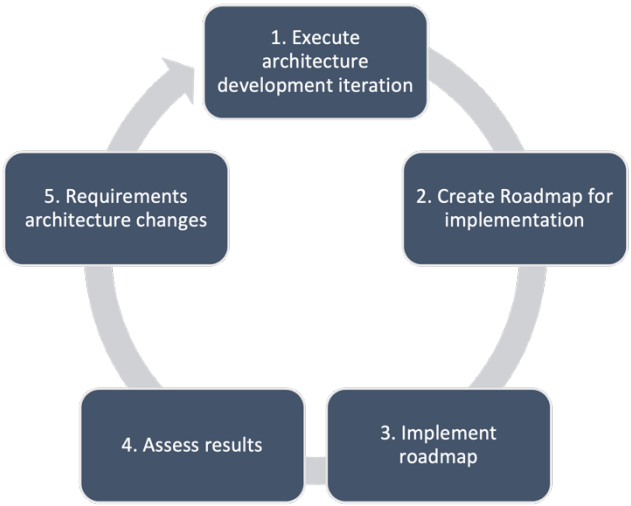


Figure 8 Architecture Development Iteration Framework

The architecture described here is developed using a custom-tailored methodology - combining world best practices with expectations and the situation in Zimbabwe. The methodology is designed for iterative use as shown in Figure 8. Also, the methodology suggests decoupling the architecture into architecture domains (see Figure 9) and describing each architecture domain by using the following concepts:

- **Architecture artefacts** - tables, lists, models or other pieces of documentation that describe the agreements and ideas developed during architecture development. Artefacts describe mostly organisational aspects that need to be adopted during architecture implementation.
- **Building blocks** - concepts that must be implemented as tangible techno-organisational solutions during architecture implementation.

The methodology and relevant frameworks are described in more detail in a separate document that should be used by the facilitators - people and organisations responsible for managing the process of architecture development and implementation.

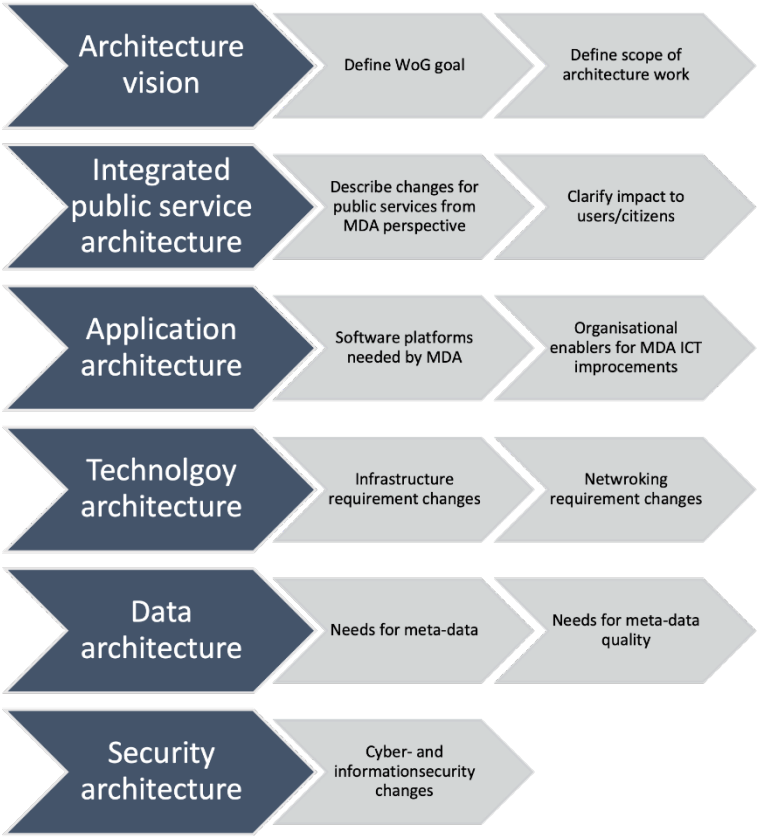


Figure 9 Architecture Domains

3 Stakeholders and Roles

For implementing a ZWoGA, in addition to the OPC, several institutions and MDAs play a crucial role, and they are seen as key stakeholders. The main stakeholder list is presented in the following. (Refer to the Appendix section for further detailed information on stakeholders and representatives from each MDA.)

- Government Internet Service Provider
- Immigration Department
- Judicial Service Commission
- Ministry of Defence
- Ministry of Energy and Power Development
- Ministry of Environment, Climate and Wildlife
- Ministry of Finance, Economic Development and Investment Promotion
- Ministry of Foreign Affairs and International Trade
- Ministry of Health and Child Care
- Ministry of Higher and Tertiary Education, Innovation, Science and Technology Development
- Ministry of Home Affairs and Cultural Heritage
- Ministry of ICT, Postal and Courier Services
- Ministry of Industry and Commerce
- Ministry of Information, Publicity and Broadcasting Services
- Ministry of Justice, Legal and Parliamentary Affairs
- Ministry of Lands, Agriculture Fisheries, Water and Rural Resettlement
- Ministry of Local Government and Public Works
- Ministry of Mines and Mining Development
- Ministry of National Housing and Social Amenities
- Ministry of Primary and Secondary Education
- Ministry of Skills, Audit and Development
- Ministry of Sports, Recreation, Arts and Culture
- Ministry of Tourism and Hospitality Industry
- Ministry of Transport and Infrastructural Development
- Ministry of Veterans of the Liberation Struggle Affairs
- Ministry of Youth Empowerment, Development and Vocational Training
- National Peace and Reconciliation Commission
- National Prosecuting Authority
- Office of the Auditor-General
- Parliament of Zimbabwe
- Postal and Telecommunications Regulatory Authority of Zimbabwe
- Procurement Regulatory Authority of Zimbabwe
- Public Service Commission
- Public Service Labor and Social Welfare

- Civil Registry Department
- Rural Infrastructure Development Agency
- TelOne
- Women Affairs, Community, Small and Medium Enterprises Development
- Zimbabwe Anti-Corruption Commission
- Zimbabwe Electoral Commission
- Zimbabwe Electricity Supply Authority
- Zimbabwe Gender Commission
- Zimbabwe Human Rights Commission
- Zimbabwe Land Commission
- Zimbabwe Media Commission
- Zimbabwe National Roads Administration
- Zimbabwe Prisons and Correctional Services
- Zimbabwe Republic Police
- Zimbabwe Revenue Authority

4 Problem & Objectives

The chapter will give an overview of why the Whole of Government Architecture is needed, what would be the short-term goal and how it is reasoned considering the current situation in Zimbabwe.

With activities from the public sector digitalization has emerged as one of the key enablers for supporting progress in society. Additionally, it has been identified that there is a stronger need to keep all MDAs in the change process to support each other. Therefore, the key phrases of the Whole of Government Architecture have been stronger digitalization and cooperation/integration of MDAs. To identify a goal from this the Whole of Government Architecture approach has been identified and will be refined into a targeted work in current and other related architecture domains deliverables.

4.1 Artefact: Concerns Catalogue

Stakeholder concerns, in the context of implementing ZWoGA, refer to the issues, challenges, or considerations that are important to various parties involved in or affected by the enterprise architecture initiatives within government organizations.

The most critical concerns identified by MDAs that require the implementation of the ZWoGA were as follows:

No.	Concerns	Description
1	Resistance to change from staff accustomed to existing processes	Current processes and public services are good enough for people working in public sector. Employees and stakeholders may be reluctant to adopt changes to systems and processes, preferring to stick with familiar methods. This resistance can hinder the implementation and reduce the effectiveness of the new approach.
2	Different digital maturity level of MDAs/Stakeholders/Experts	MDAs along with other stakeholders and experts, may have varying levels of experience and readiness for adopting new ICT frameworks. This disparity can lead to inconsistencies and challenges in achieving a unified approach and reduce willingness to cooperate between MDAs.
3	Difficulty in integrating existing legacy systems	Many Government entities are relying on outdated or legacy systems that are not compatible with modern ICT infrastructure and not intended for integrations.

No.	Concerns	Description
		Integrating these old systems (with new ones or between themselves) can be complex and costly and further limits the capability of making significant cooperation between MDAs.
4	Lack of a clear communication plan regarding new whole of government approach with its milestones and progress	Effective implementation requires close coordination among various Government entities. A lack of coordination between MDAs can result in duplicated efforts, misaligned goals, and inefficient use of resources.
5	Lack of skilled (IT) staff to manage and maintain ICT solutions.	There may be insufficient technical skills, financial resources, and human capacity to support the implementation and maintenance of the new ZWoGA. Building the necessary capacity is crucial for the successful deployment and operation of the enterprise architecture.

Refer to the appendix section for a further comprehensive list of concerns catalogue. It is expected that upon following iterations of the architecture work the concerns list is revised and key concerns that must be addressed are brought up for resolution.

4.2 Artefact: List of Change Drivers & Opportunities

Several strengths make the Zimbabwean government well-positioned to implement ZWoGA and achieve ZWoGA's goal to ensure driving a smooth digital transformation and improving the quality and accessibility of public services for citizens. Several heightened strengths that have been identified during preliminary situation analysis and discussions with stakeholders are as follows:

- **Commitment to improve the provision of public services by ICT governance-related entities**. Institutions such as the OPC and the Ministry of ICT, Postal and Courier Services (MICTPCS) have shown a strong dedication to enhancing public service delivery through improved ICT governance. This dedication and commitment are reflected in different initiatives such as the formulation and implementation of policies, and frameworks aimed at improving the efficiency of public services.
- **Motivated leadership to support digital transformation**. There is proactive and motivated leadership in the government at various levels and across all MDAs. Leaders who understand the importance of digitalization,

innovation, and modernizing government operations, and are actively supporting initiatives that drive changes.

- **Existence of minimal infrastructure in the public sector and fast consumption of the resources at MDAs**. While currently there might be minimal infrastructure in place, yet this can be seen as a strength because it provides a foundation for implementing scalable and integrated solutions. The rapid consumption of resources at MDAs indicates the need for efficient and optimized systems and shows a great will to digitalize public services.
- **Public demand for improved services**. There is a notable and growing expectation from the public towards more efficient services. This demand is seen as a strong driver for change and implementation of advanced ICT solutions.
- **MDA demand for digital enablement**. MDAs are increasingly seeking digital solutions that enable efficient data exchange, secure digital authentication, and other horizontal platforms. This demand is seen as a strength as it demonstrates the understanding of the advantages of digital enablement to ensure providing better services to citizens.

4.3 Artefact: Vision and Goal

The vision of (ZWoGA) defines the expected future state and long-term aspirations for the Government that empowers ICT, what the Government wants to achieve through ICT and serves as a guideline for managing and leveraging ICT resources and decisions. The (ZWoGA) goal agreed by MDAs is

Providing a strategic framework for aligning and integrating Government ICT infrastructure and systems.

This goal is directly linked to providing better services for citizens by establishing an integrated ICT infrastructure that improves the efficiency, transparency, and accessibility of public services. Moreover, this goal enables the government to more effectively address citizens' needs.

What does the ZWoGA goal mean?

1. Strategic Framework for having a clear set of guidelines, methodologies, standards and best practices for developing, implementing and managing ICT resources, infrastructure, and systems in Zimbabwe.
2. Alignment for ensuring that the ICT initiatives and projects across all MDAs are aligned with the overall strategic objectives of the Zimbabwean Government

and providing a clear Roadmap and directions for ICT resources and prioritization of projects.

3. Integration of MDAs from various aspects for ensuring cooperation, interoperability and data sharing among MDAs using a standardized approach.
4. MDAs must be provided with a set of tools that enable faster and more effective development of public services and cooperation with other MDAs.
5. All the above-described changes of work are introduced to ensure better satisfaction of end-users - citizens and entrepreneurs.

What ZWoGA goal does not mean?

The goal does not support the following:

1. Ad-hoc implementation of fragmented ICT projects that do not align with the Whole of Government's strategic goals.
2. Short-term fixes or temporary solutions that do not consider future scalability and integration needs.
3. Introduction of solutions without recognizing its maintenance and operational needs and manpower.
4. Freedom to choose and apply whatever standard, protocol, methodologies, or practices by any stakeholder where it has an impact on other stakeholders.
5. Unmanaged or isolated management of ICT infrastructure and systems.
6. Independent decision-making at each MDA on aspects that impact other MDAs.

4.4 Artefact: Objectives of Architecture

ZWoGA plays a vital role in providing a strategic framework for the alignment and integration of Government ICT infrastructure and systems, addressing key concerns such as resistance to change, obsolete and legacy systems, lack of coordination, and capacity limitations. By establishing clear principles, standards, and guidelines, ZWoGA facilitates a cohesive approach to ICT development, ensuring that all Government entities move towards common goals and objectives.

This unified Architecture helps in overcoming resistance to change by providing a clear Roadmap and benefits that justify the transformation efforts.

Additionally, ZWoGA promotes the modernization of outdated systems by prioritizing interoperability and phased upgrades, thereby gradually replacing legacy systems without causing significant disruptions to ongoing operations. ZWoGA fosters improved coordination and collaboration among different departments and agencies, breaking down silos and enabling seamless data sharing and communication. This enhanced coordination is essential for addressing capacity limitations, as it allows for the optimal utilization of resources and expertise across the government.

By leveraging the strengths of various MDAs, ZWoGA creates opportunities for innovation and efficiency gains, ultimately leading to more effective and responsive government services.

Additionally, the ZWoGA as a strategic framework encourages the adoption of emerging technologies and best practices, ensuring that Government ICT infrastructure remains robust, scalable, and capable of meeting future demands. This proactive approach not only mitigates current challenges but also positions the Zimbabwean Government to take advantage of new opportunities, driving continuous improvement and better service delivery for citizens.

4.5 Artefact: Risks Catalogue

A risk in implementing ZWoGA refers to any potential event or circumstance that could negatively impact the successful execution or outcomes of Enterprise Architecture initiatives within Government organizations. These risks may arise from various sources, identifying, assessing, and mitigating these risks is essential for minimizing disruptions and maximizing the effectiveness of government enterprise architecture efforts.

Risk mitigation in implementing ZWoGA involves taking proactive measures to reduce or eliminate the potential negative impacts of identified risks on the success of Enterprise Architecture initiatives. By addressing risks early and effectively, organizations can minimize disruptions, enhance resilience, and increase the likelihood of achieving their enterprise architecture objectives.

Agreed risks by MDAs toward implementing the ZWoGA are presented in the table below.

No.	Risk	Potential Impact	Potential Mitigation Approach
1	Lack of Stakeholder buy-in	Without the support and commitment of key stakeholders, the implementation of the Enterprise Architecture can face significant obstacles. Stakeholder resistance can lead to delays, reduced cooperation, and ultimately, failure to achieve the intended benefits. This lack of buy-in can undermine the entire initiative, resulting in wasted resources and missed opportunities for improvement.	Develop a comprehensive communication strategy to inform stakeholders about the benefits and goals of the Enterprise Architecture. Regularly update them on progress and involve them in decision-making processes. Conduct training sessions and workshops to demonstrate the value of the new architecture and address any concerns or misconceptions.
2	Insufficient funding and resources allocated to the project	Inconsistent or inadequate funding can halt progress, lead to incomplete projects, and reduce the quality of implementations. This financial instability can compromise the effectiveness and sustainability of the Enterprise Architecture, leaving systems fragmented and outdated.	Develop a detailed and realistic budget plan that covers the entire implementation period and secures commitment from relevant authorities. Explore multiple funding sources, including Government designated budget, grants, partnerships, and public-private collaborations, to ensure a steady flow of resources. Establish strong financial oversight mechanisms to manage and allocate funds efficiently.
3	Inadequate skills of end-users	End-users with insufficient skills may struggle to effectively use new systems, leading to reduced productivity, errors, and frustration. This skill gap can diminish the overall impact of the Enterprise Architecture and hinder the achievement of its objectives.	Implement comprehensive training programs tailored to the needs of different user groups. These should include hands-on practice, tutorials, and ongoing support. Ensure that the systems are designed to be intuitive and user-friendly, minimizing the learning curve for end-users.

No.	Risk	Potential Impact	Potential Mitigation Approach
			Establish help desks and support systems to assist end-users with any issues or questions they may have.
4	Inadequate skills of Government Employees	A lack of skilled Government Employees and high turnover rates can disrupt the continuity and stability of the Enterprise Architecture implementation. This can lead to knowledge loss, inefficiencies, and increased costs due to repeated training and onboarding.	Invest in continuous professional development programs to enhance the skills of Government Employees. Focus on upskilling in relevant technologies and processes. Implement strategies to improve employee retention, such as offering competitive salaries, career advancement opportunities, and a positive work environment. Develop robust knowledge management systems to capture and retain critical knowledge, ensuring that it is accessible to new employees.

Refer to the appendix section for a further comprehensive list of risks catalogue.

4.6 Artefact: Metrics and KPI

Key Performance Indicator (KPI) is a metric that's used to measure the progress and success of an organization or a specific activity. KPIs help to quantify the achievement of important business objectives and provide a basis for decision-making and improvement. For Zimbabwe the KPIs must be agreed upon by stakeholders through finding what can be measured and what exposes the progress of architecture implementation the best way.

The agreed KPIs by MDAs to be used for measuring the ZWoGA were as follows:

Table 5 KPIs

No.	KPI	Description
1	Customer Satisfaction	Zimbabwean Government can use customer satisfaction as a KPI to ensure that Government services meet or exceed the expectation of citizens through measuring the level of satisfaction this can include collecting information through user surveys, feedback forms, and user satisfaction ratings.
2	Citizens accessing digital services	Zimbabwean Government can use citizens accessing digital services as a KPI to evaluate the effectiveness and reach of digital transformation initiatives and to track the number of citizens using digital services provided by the government. The assessment can be done through measuring number of frequency of access to services and the percentage of the population using digital services.
3	Uptime (systems and servers)	Zimbabwean Government can use uptime (systems and servers) as a KPI to measure the availability and reliability of IT systems and servers and ensure that government services are accessible and functional when needed. The assessment can include measuring percentage uptime, mean time between failures and mean time to repair.
4	Recovery time	Zimbabwean Government can use recovery time as a KPI to measure the time taken to restore public services after an outage or failure to assess the efficiency and effectiveness of disaster recovery and business continuity plans. The assessment can include measuring mean time to recovery (MTTR) and recovery

No.	KPI	Description
		point objective (RPO) to measure the maximum amount of data loss.
5	Revenue growth	Zimbabwean Government can use revenue growth as a KPI to track the increase in revenue generated through Government services and operations, and to evaluate the financial performance and sustainability of Government initiatives. The assessment can be done through measuring the percentage growth in revenue, yearly comparison, and revenue from new services.

The KPI needs to be refined and specified into measurable units by the ICT-governing entities.

Refer to the appendix section for a further comprehensive list of KPIs catalogue.

5 Environment and Process

In the current environment, as presented in Figure 10, public service processes are maintained through fragmented systems, causing significant challenges for citizens who are seeking public services. The figure represents a citizen interacting with three MDAs where each MDA has its own procedures and front office (green part), some information system supporting its back-office work (blue part) and some infrastructure to make it all work (black part). When citizens need to obtain these services, they are required to visit multiple MDAs - relevance identified by citizens - and repeatedly submit data and

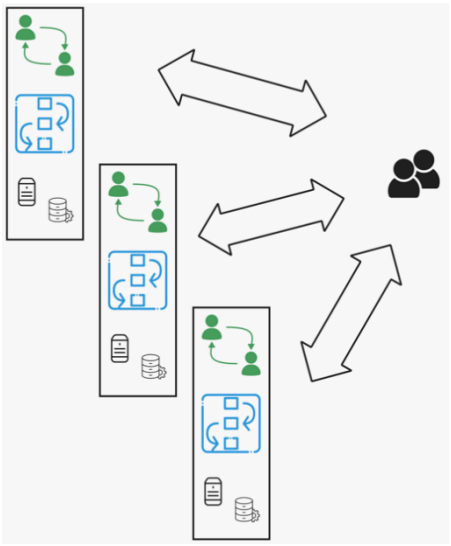


Figure 10 Obtaining public services in the current environment

carry certificates and proof from one authority to another. Additionally, the responsibility of data collection falls on the citizens themselves. This model is associated with numerous challenges, including data inconsistency and quality, time consumption, additional administrative costs, risk of corruption, and an overall lack of transparency and efficiency in obtaining public services.

This fragmented approach leads to significant inefficiencies and frustrations for citizens. Data inconsistency arises because different MDAs may have varying information for the same individual, leading to errors and delays. The process is time-consuming, as citizens must navigate through multiple offices and repeat their submissions. This not only wastes time but also demands extra costs, such as travel expenses and lost productivity. Moreover, the current model lacks the transparency of processes as in most cases the public service is provided by humans in the front office even if some level of back office is digitized. Citizens often have little visibility into the status of their requests, leading to

uncertainty and dissatisfaction. The approach is also inefficient, as it does not leverage modern technologies to streamline processes and improve service delivery.

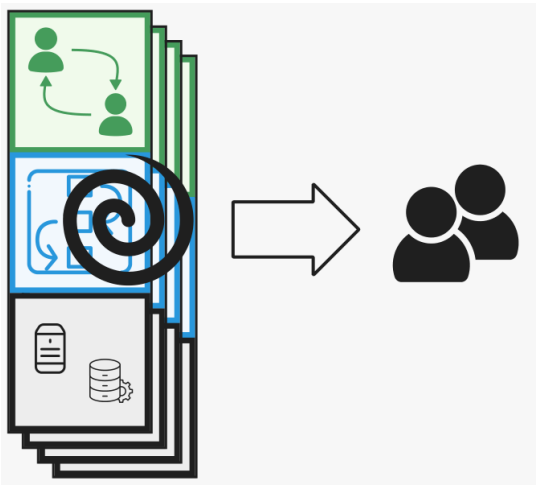


Figure 11 Integrated public services

Transitioning to a digitalized and integrated public service model as shown in Figure 11, presents a transformative solution to the existing challenges. While MDAs preserve their processes (green part), custom information systems (blue part) and some infrastructure (black part) they are aligning their resources and cooperating in the provision of public services. Ensuring that citizens only need to submit their information once, which is then accessible to all relevant MDAs, the entire public service provision becomes significantly more streamlined and efficient when MDAs have interoperable systems, data can be submitted once and reused by all necessary agencies, eliminating the need for repeated submissions. This expects strong cooperation between the MDA processes (green part on diagram) and information systems (blue part in diagram). Recognizing each other infrastructure limitations (black part on the diagram) is also highly relevant.

This shift would enhance data consistency, as the same accurate information would be utilized across all platforms, reducing errors and discrepancies. The time saved from not having to visit multiple offices or repeatedly submit data would be substantial, allowing citizens to dedicate their time to more productive activities. Additionally, reducing redundant processes would result in significant cost savings for both citizens and the government.

As key challenges, the following have been identified by MDAs as bottlenecks: insufficient network coverage, lack of ICT-related skills in MDAs to create better ICT solutions, no means for secure authentication of citizens in digital environments, and no joint way for exchanging data between MDAs. These tools would secure transactions and interactions within the digital system and between MDAs. This enhanced security would build trust among citizens, assuring them that their data is handled safely and responsibly.

Overall, implementing a digitalised and integrated public service model would create a more transparent and efficient system for obtaining public services. It would foster a seamless experience for citizens, where services are delivered more quickly, accurately, and transparently. This modernization would represent a significant step forward in public administration and improving the quality of life for all Zimbabwean citizens.

6 High-level Target Architecture

The integrated public services approach relies on two principal changes from the citizen perspective:

1. MDAs cooperate to provide a better-aligned experience of public services for citizens.
2. MDAs primarily deliver public services via digital channels through their information systems, occasionally adopting a "digital by default" approach.

While those changes are highly MDA-specific, it must be acknowledged that in Zimbabwe MDAs alone may not be able to adopt such changes effectively. Therefore, to foster expected change and achieve the desired transformation, a series of Architecture domains are established to structure and assist the MDAs, making it easier for them to adopt the Integrate Public Service approach.

The Key domains addressed by the Zimbabwean Whole of Government Architecture (ZWoGA) are (presented also on Figure 7):

1. **Integrated public service architecture** - assists public service owners in designing or redesigning their public services to benefit digitalization and provide better public services for citizens. As the functional complexity in each MDA is very specific, this will be respected as something that an MDA and its service owners must implement internally to be able to create the best systems for the best public service.
2. **Application Architecture** - provides a set of common functionalities as techno-organisation platforms that ease the burden of creating interoperable information systems in each MDA.
3. **Technology Architecture** - ensures adequate infrastructure, communication and other baseline IT services to be operational from the MDAs on demand.
4. **Data Architecture** - provides an overview of the capabilities of other MDAs to understand how and with whom cooperation can be done (process and data sharing capabilities in specific).
5. **Security Architecture** - suggests a standardised approach for implementing security measures and emergency response capabilities to keep MDAs and their information systems security aware.
6. **Governance Architecture** – encompasses ICT governance and facilitation services to ensure that all architecture domains are aligned.

It is important to recognize that inter-agency cooperation among MDAs is not common practice in Zimbabwe. Therefore, the implementation of ZWoGA should be kept as straightforward as possible. The role and positions of MDA staff should not undergo drastic changes, and any modification to existing responsibilities and work distribution

between MDAs, OPC and MICTPCS should be adjusted with careful consideration and tact. Given that there are six architecture domains, MDAs may perceive the changes as significant and dramatic even if each domain and its corresponding building blocks only introduce slight alternations to the current workflow. This perception of substantial change must be acknowledged and addressed effectively, particularly, at the Governance Architecture level.

6.1 Principles

Principles are fundamental guidelines that shape the design and implementation of a Whole of Government Enterprise Architecture. EA baseline principles:

- Define the general rules and guidelines for the use and deployment of all IT resources and assets.
- Reflect a level of consensus among the various elements.
- Form the basis for making future IT decisions.

Agreed principles by MDAs to be established as a first phase to support the implementation of ZWoGA were as follows:

Table 6 Architecture Principles

No.	Principle	Description
1	Data Privacy, Authenticity, and Integrity is guaranteed	This principle is to ensure that all data handled by Government systems is protected against unauthorized access, tempering and lose. As well as, to protect citizens' information and ensuring that data is kept confidential, accurate, and reliable.
2	Service Delivery follows User-Centric Approach	This principle is to ensure that Government services are designed around the needs and experiences of the users. To make Government services more accessible, efficient, and satisfactory for citizens.
3	Users must provide same data to Government only once	This principle is to ensure that citizens do not provide same information repeatedly to different MDAs. This is to reduce redundancy and administrative burden on citizens, enhancing efficacy and user experience.
4	Solutions are easily Scalable for high Availability and Reliability	This principle is to ensure that IT solutions designed to handle increasing workloads and services are

No.	Principle	Description
		always available. Additionally, it aims to ensure that government services are reliable and can handle peak demands without distribution.
5	Development Processes and Standards enforce Quality and Security	This Principle is to ensure that all ICT development follows strict Standards for Quality and Security to have Robust, Secure, and high Performing Government Systems.
6	Continuous Funding is guaranteed for maintenance, development and evolution	This Principle is to ensure that there is a consistent financial support for the uptake and advancement of government IT systems. Moreover, to prevent service disruptions and allow for continues investments to maintain and evolve IT infrastructure.
7	Innovation and Emerging Technologies are used	This Principle is to ensure that new Technologies and Innovative approaches are adopted in developing Government Systems to enhance the efficiency, responsiveness, and effectiveness of public services.
8	Administrative Processes, Service Provision, Data Management and Decision-Making are transparent	This Principle is to ensure that Government operations are open and accessible to public. To build trust and accountability in Government actions and decisions through open data initiatives, public reporting, and clear communication channels.

At the Governance Architecture level, a control mechanism must be put in place at a suitable level of empowerment to ensure that the principles are followed by each stakeholder.

Refer to the appendix section for a further comprehensive list of principles catalogue.

6.2 Policies

Policy is a set of Principles, Guidelines, or Rules established by an organization, Government, or authority to guide decision-making, actions, and behaviours within a specific context or area of operation.

Agreed policies by MDAs to be established as a first phase to support the implementation of ZWoGA were as follows:

Table 7 Generic Policies to Support ZWoGA

No.	Policies	Description
1	Enterprise Architecture Policy	This Policy aims to provide the overarching principles, objectives, and governance framework for enterprise architecture development and implementation
2	IT Governance Policy	This Policy aims to define the governance structure, roles, and responsibilities for IT decision-making, investment prioritization, and project oversight.
3	Information Security Policy	This Policy aims to establish rules and procedures for protecting Government information assets from unauthorized access, disclosure, alteration, and destruction.
4	Disaster Recovery and Business Continuity Policy	This Policy aims to establish plans and procedures for recovering from system failures, data breaches, and other disruptions to government operations.
5	Password Policy	This Policy aims to define guidelines and requirements for creating and managing passwords to ensure their strength and security. Protects sensitive information and systems by ensuring that passwords are difficult to guess or crack, thereby preventing unauthorized access.
6	Bring Your Own Device (BYOD) Policy	This Policy aims to establish rules and procedures governing the use of personal devices, such as smartphones, tablets, and laptops, for accessing government IT systems and data. This policy allows the convenience of using personal devices while ensuring that security and compliance requirements are met to protect sensitive Government information.

Refer to the appendix section for a further comprehensive list of policies catalogue.

7 Appendices

7.1 Concerns Catalogue

Table 8 Catalogue of Concerns

No	Concerns	Classifier
Cost and Disruption		
1	High upfront costs for planning, technology, and training.	Impacted
2	Uncertain return on investment on the EA project.	Future
3	Disruption to daily operations and service delivery during implementation.	Impacted
4	Increased workload for staff during the transition.	Impacted
5	Potential for cost overruns due to unforeseen technical challenges.	Impacted
6	Lack of funding for ongoing maintenance and upgrades of the EA.	Impacted
7	Security risks associated with data migration and integration.	Impacted
8	Potential for data loss during system transitions.	Impacted
9	Hidden or underestimated costs associated with change management.	Impacted
10	Inequitable distribution of costs across different Government agencies.	Impacted
11	Potential for delays in project completion impacting service delivery.	Impacted
12	Long-term financial commitment required to maintain the EA.	Future
Change Management and Silos		
13	Resistance to change from staff accustomed to existing processes.	Addressed
14	Loss of departmental autonomy and control over IT systems.	Addressed

No	Concerns	Classifier
15	Standardized solutions not meeting the specific needs of individual agencies.	Impacted
16	Difficulty in integrating new systems with existing legacy systems.	Addressed
17	Ineffective communication regarding project goals and benefits.	Addressed
18	Lack of training or support for staff adapting to new workflows.	Addressed
19	Unclear definition of roles and responsibilities within the EA framework.	Impacted
20	Concerns about siloed decision-making hindering collaboration across agencies.	Impacted
21	Lack of trust between agencies regarding data sharing and security.	Impacted
22	Limited opportunities for stakeholder feedback throughout the implementation process.	Future
23	Resistance from senior management who are comfortable with existing systems.	Impacted
24	Potential for employee morale to decline due to change fatigue.	Impacted
25	Difficulty in managing cultural differences across various government departments.	Future
Technical Concerns		
26	Technical complexity of integrating disparate systems across government bodies.	Impacted
27	Compatibility issues between existing systems and the new EA platform.	Impacted
28	Data security vulnerabilities introduced through integration.	Impacted
29	Lack of skilled IT staff to manage and maintain the EA infrastructure.	Addressed
30	Potential for system downtime or outages during implementation.	Future

No	Concerns	Classifier
31	Concerns about the scalability of the EA to accommodate future growth.	Future
32	Limited flexibility within the EA to adapt to emerging technologies.	Future
33	Lack of robust disaster recovery plan for the EA infrastructure.	Future
34	Concerns about the ongoing technical support available for the platform.	Impacted
35	Difficulty in ensuring data quality and consistency across the EA.	Future
36	Lack of user-friendly interfaces for the EA systems.	Impacted
37	Difficulty in measuring the long-term benefits of the EA project.	Impacted
38	Unrealistic expectations regarding the speed of achieving EA benefits.	Impacted
39	Lack of a clear communication plan regarding project milestones and progress.	Addressed
40	Concerns about the long-term sustainability of the EA.	Impacted
41	Limited involvement of stakeholders in defining project goals and solutions.	Addressed
42	Lack of a plan for ongoing EA improvement and innovation.	Addressed
43	Difficulty in quantifying the cost savings achieved through implementing the EA.	Future
44	Potential for the EA to become outdated without regular updates.	Impacted
45	Concerns about the environmental impact of implementing and maintaining the EA.	Future
46	Difficulty in demonstrating the EA's positive impact on citizen services.	Impacted
47	Lack of mechanisms to ensure EA aligns with future Government priorities.	Impacted

No	Concerns	Classifier
48	Difficulty in attracting and retaining skilled IT staff for EA maintenance.	Impacted
49	Concerns about the EA becoming overly complex and bureaucratic.	Impacted
50	Limited focus on user experience when designing and implementing the EA.	Addressed
51	Different digital maturity levels of MDAs/Stakeholders/Experts	Addressed

7.2 Risks Catalogue

Table 9 Catalogue of Risks

No	Risk	Mitigation approach	Impact
1	Lack of stakeholder buy-in and support	Engage stakeholders early and continuously throughout the process, communicate the benefits clearly, and address their concerns proactively.	High
2	Insufficient funding and resources allocated to the project	Conduct a thorough cost-benefit analysis, secure adequate funding upfront, and prioritize resource allocation based on critical project needs.	High
3	Complexity of integrating diverse systems and platforms	Break down the integration process into manageable phases, establish clear integration standards and protocols, and leverage middleware or integration tools to streamline the process.	
4	Inadequate technical expertise and capacity within the organization	Invest in training and skill development for existing staff, recruit experienced professionals if necessary, and establish partnerships with external consultants or vendors with the required expertise.	
5	Resistance to change from employees and leadership	Develop a comprehensive change management plan, communicate the vision and benefits of the architecture, involve employees in decision-making	

No	Risk	Mitigation approach	Impact
		processes, and provide support and training to facilitate adoption.	
6	Data Security breaches and Cybersecurity threats	Implement robust Cybersecurity measures, including encryption, access controls, and regular security audits, establish incident response protocols, and educate employees about security best practices.	
7	Incompatibility with existing legacy systems	Conduct a thorough assessment of existing systems, prioritize integration or migration efforts based on business needs, and consider phased approaches or interim solutions to bridge compatibility gaps.	
8	Poor data quality and integrity	Implement data quality management processes, establish data governance frameworks, conduct regular data audits, and invest in data cleansing and validation tools.	
9	Failure to meet regulatory compliance requirements	Stay informed about relevant regulations and standards, conduct compliance assessments, establish clear policies and procedures, and engage legal experts to ensure adherence to legal requirements.	
10	Lack of alignment with organizational goals and priorities	Align architecture initiatives with strategic objectives, involve key stakeholders in the planning process, regularly reassess alignment with evolving priorities, and adjust plans accordingly.	
11	Scope creep leading to project delays and cost overruns	Define clear project scope and deliverables upfront, establish change control processes, monitor progress closely, and prioritize requirements based on business value and feasibility.	
12	Ineffective Change Management processes	Develop a comprehensive Change Management strategy, identify and address potential resistance early, provide training and support to affected	

No	Risk	Mitigation approach	Impact
		stakeholders, and communicate changes transparently.	
13	Legal and regulatory challenges related to data privacy and governance	Stay abreast of relevant laws and regulations, conduct privacy impact assessments, implement privacy-by-design principles, and establish clear policies and procedures for data handling and governance.	
14	Difficulty in achieving Interoperability among different government agencies	Establish Interoperability Standards and Protocols, promote data sharing agreements and API development, establish governance bodies to oversee interoperability efforts, and invest in interoperability testing and validation.	
15	Inadequate skills of Government employees	Develop comprehensive training programs tailored to different roles and skill levels, provide ongoing learning opportunities, and encourage knowledge sharing and collaboration among staff members.	High
16	Dependence on external vendors and service providers	Diversify vendor relationships, establish clear service level agreements (SLAs) and performance metrics, conduct regular vendor assessments, and maintain contingency plans for vendor failures or disruptions.	
17	Loss of institutional knowledge during the transition process	Document critical knowledge and processes, establish knowledge transfer mechanisms, mentor new staff members, and maintain continuity through phased transitions or overlap periods.	
18	Insufficient testing and quality assurance procedures	Develop comprehensive testing plans, conduct thorough system and integration testing, involve end users in user acceptance testing (UAT), and prioritize quality assurance throughout the project lifecycle.	

No	Risk	Mitigation approach	Impact
19	Inaccurate or incomplete documentation of architecture components	Establish clear documentation standards and templates, assign responsibility for documentation tasks, conduct regular reviews and updates, and ensure documentation is accessible and well-organized.	
20	Resistance from external stakeholders or partners	Engage external stakeholders early and involve them in decision-making processes, address their concerns and priorities, establish clear channels for communication and collaboration, and build trust through transparency and accountability.	
21	Inadequate skills of end-users.		High

7.3 KPI Catalogue

Table 10 Catalogue of KPIs

No.	KPI	Classifier
Financial KPIs for the Government		
1	Budgeting ratio (Government revenue, Government operating cost, and Revenue per capita)	Addressed
2	Near-term solvency (Debt per capita)	
3	Personnel and admin cost ratio	
4	Bond rating	
Operational KPIs for the Public Sector		
5	Regulatory practices quality	
6	Total number of Audit findings	
Service KPIs for the Government		

No.	KPI	Classifier
7	Housing KPIs (measure of housing affordability, Number of chronically homeless individuals)	
8	Environmental KPIs (Passenger trips on buses per gallon of fuel, Landfill diversion rate)	
9	Infrastructure KPIs (Total miles of municipal streets paved, Percentage of bridges with a sufficient rating, and Capital projects timely and on-budget completion)	
10	e-Government Infrastructure KPIs (Capacity, Accessibility, Interconnectivity and Interoperability, and Security)	
Citizen KPIs for Public Sector		
11	Public participation	
12	Voter turnout	
13	Resident satisfaction	Addressed
Human Resources KPIs for the Government		
14	Diversity of workforce	
15	Employee retention rate	

7.4 Architecture Principles Catalogue

Table 11 Catalogue of Principles, Extended

No	Principles	Classifier
Interoperability underlying principles		
1	Administrative processes, service provision, data management and decision-making are transparent (transparency).	Addressed
2	Existing interoperability solutions, tools, components etc. are reusable (sustainability).	

No	Principles	Classifier
3	Information systems and services do not depend on specific technology (tech-neutrality).	
4	Data is portable across services (reusability).	
5	Service delivery follows user-centric approach (user-centric).	Addressed
6	Everyone can access public services (accessibility).	
7	Interaction with the Government is secure and trustworthy (security).	
8	Data privacy, authenticity, and integrity is guaranteed (security).	Addressed
9	Administrative processes are simple and provide value (user-centric).	
10	Information is preserved for reuse (accessibility).	
11	Service delivery is effective and efficient (user-centric).	
12	Government decisions are taken as closely as possible to the citizens(user-centric).	
13	Data is shared with other decision makers (reusability).	
Digital Public Service Strategy Principles		
14	End-user services are digital by default (accessibility).	
15	Service development enables data-driven decision making (reusable).	
16	Government and Civil Servants anticipate users' needs (proactiveness).	
17	Users are engaged into ICT related decision making (transparency).	
Digital Public Service Design Principles		

No	Principles	Classifier
18	Users must provide same data to Government only once (reuse).	Addressed
19	Users' needs are put at the centre (user-centric).	
20	Service design follows proactive approach (user-centric).	
Digital Public Service Operations		
21	Public services development follows security by design principle (security).	
22	Information is preserved for reuse and validation (accessibility).	
Solution Architecture Principles		
23	Open standards are used (open).	
24	Built and created software is open source (open).	
25	Solutions are cloud native (open).	
26	Continuous funding is guaranteed for maintenance, development and evolution (sustainability).	Addressed
27	Microservices-based Architecture is used (sustainable).	
28	Development processes and standards enforce quality and security (secure).	Addressed
29	Solutions are regularly scanned and audited (security).	
30	Public reviews help to achieve security (security).	
31	Services meet users where they are (accessibility).	
32	Development process is open to community contributors (accessibility).	
33	Resource needs for solutions are minimized (power, bandwidth, unreliable connectivity) (robust).	

No	Principles	Classifier
34	Solutions are easily scalable for high availability and reliability (robust).	Addressed
35	Decoupling is based on API-only (robust).	
36	Innovation and emerging technologies are used (accessibility).	Addressed

7.5 Policies Catalogue

Table 12 Catalogue of Policies, Extended

No	Policy	Description	Classifier
1	Enterprise Architecture Policy	Provides the overarching Principles, objectives, and governance framework for enterprise architecture development and implementation.	Addressed
2	Data Governance Policy	Defines Standards, Guidelines, and Processes for managing Government data, including quality, security, privacy, and lifecycle management.	
3	Information Security Policy	Establishes rules and procedures for protecting government information assets from unauthorized access, disclosure, alteration, and destruction.	Addressed
4	Privacy Policy	Protects the privacy rights of citizens by establishing rules and safeguards for the collection, use, and disclosure of personal information by Government agencies.	
5	Open Data Policy	Promotes transparency and accessibility by establishing guidelines for the publication and sharing of Government data in open and machine-readable formats.	
6	Interoperability Policy	Promotes interoperability among Government systems, applications, and services by defining standards, protocols, and interfaces for data exchange and integration.	

No	Policy	Description	Classifier
7	IT Governance Policy	Defines the Governance structure, roles, and responsibilities for IT decision-making, investment prioritization, and project oversight.	Addressed
8	Technology Standards Policy	Sets standards and specifications for technology infrastructure, platforms, and solutions to ensure compatibility and sustainability.	
9	Change Management Policy	Outlines the process for managing changes to the Enterprise Architecture, including requirements gathering, impact assessment, and stakeholder communication.	
10	Data Sharing and Collaboration Policy	Facilitates the sharing and collaboration of data among Government agencies and external stakeholders while protecting sensitive information and privacy rights.	
11	Enterprise Data Architecture Policy	Defines the structure, semantics, and relationships of Government data assets to enable effective data management and utilization.	
12	Cloud Computing Policy	Establishes guidelines and best practices for the adoption, deployment, and management of cloud-based services and solutions.	
13	Application Development and Maintenance Policy	Governs the development, deployment, and maintenance of Government applications to ensure consistency and quality.	
14	Service-Oriented Architecture Policy	Promotes the design and implementation of modular, reusable services to support agile and interoperable Government systems.	
15	Enterprise Risk Management Policy	Establishes processes and procedures for identifying, assessing, and managing risks associated with Enterprise Architecture initiatives.	

No	Policy	Description	Classifier
16	Digital Identity Policy	Defines standards and protocols for managing digital identities and authentication mechanisms to ensure secure access to Government services and information.	
17	Accessibility Policy	Ensures that government digital services and platforms are accessible to all citizens, including those with disabilities, by adhering to accessibility standards and guidelines	
18	Data Quality Policy	Sets criteria and procedures for ensuring the accuracy, reliability, and consistency of government data to support informed decision-making and analysis.	
19	Business Process Management Policy	Governs the design, documentation, and optimization of Government business processes to enhance efficiency and effectiveness.	
20	Cybersecurity Incident Response Policy	Outlines the steps and procedures for detecting, responding to, and recovering from Cybersecurity incidents to minimize the impact on Government operations and data.	
21	Digital Preservation Policy	Ensures the long-term preservation and accessibility of digital Government records and assets through proper storage, backup, and archival practices.	
22	Performance Measurement and Evaluation Policy	Establishes metrics, benchmarks, and reporting mechanisms for assessing the effectiveness, efficiency, and impact of Enterprise Architecture initiatives on Government operations and service delivery.	
23	IT Investment Management Policy	Establishes criteria and processes for prioritizing and evaluating IT investments to maximize value and alignment with strategic objectives.	
24	Information Lifecycle	Defines processes and procedures for managing the lifecycle of Government information from	

No	Policy	Description	Classifier
	Management Policy	creation to disposal, including storage, retrieval, and archiving.	
25	Training and Awareness Policy	Provides guidelines and resources for educating Government employees and stakeholders about Enterprise Architecture concepts, principles, and best practices.	
26	Records Management Policy	Ensures the proper creation, maintenance, and disposal of Government records in accordance with legal and regulatory requirements.	
27	Disaster Recovery and Business Continuity Policy	Establishes plans and procedures for recovering from system failures, data breaches, and other disruptions to Government operations.	Addressed
28	Procurement and Vendor Management Policy	Defines processes and criteria for procuring technology products and services and managing relationships with vendors.	
29	Mobile Device Management Policy	Sets rules and procedures for managing and securing mobile devices used by Government employees to access enterprise systems and data.	
30	Compliance and Regulatory Policy	Ensures compliance with relevant laws, regulations, and standards governing enterprise architecture, data management, privacy, and security.	
31	Password Policy	Defines guidelines and requirements for creating and managing passwords to ensure their strength and security. Protects sensitive information and systems by ensuring that passwords are difficult to guess or crack, thereby preventing unauthorized access.	Addressed
32	Bring Your Own Device (BYOD) Policy	Establishes rules and procedures governing the use of personal devices, such as smartphones, tablets, and laptops, for accessing government IT	Addressed

No	Policy	Description	Classifier
		systems and data. This Policy allows the convenience of using personal devices while ensuring that security and compliance requirements are met to protect sensitive Government information.	

7.6 Stakeholders Details

Table 13 Stakeholder Details

No	MDA	Name	Designation
1	Office of the President and Cabinet, e-Government Technology Unit	Dr. Tafara. Matekaire	Permanent secretary
		Tawanda. Tagwireyi	Chief Director
		Edmore Muguna	Director Projects
		Tonderai Mangono	Director Enterprise Systems
		Mackenzie Jambabwo	Deputy Director Infrastructure Support Engineering
		Katherine Hamamiti	Deputy Director Network Support Engineering
		Alice Benhura	Deputy Director Network Security Operations Centre
		Wadzanai Chihope	Deputy Director Projects
		Ignatius Majange	Deputy Director Operations
2	Women Affairs, Community, Small and Medium Enterprises Development	Advocate P. P. Sibanda	ICT Officer
		Brian Guyo	A/Deputy Director Women Empowerment

No	MDA	Name	Designation
3	Zimbabwe Human Rights Commission	Thabani Shoko	Registrar of Cooperatives
		V.J Sibanda	Deputy Director: ICT
		C. Tanyanyiwa	Director: Finance and Administration
3	Office of the Auditor-General	J. Jenya	Deputy Director Administration
		Tauji Mamwadi	Systems Manager
		Vongai Shiri	Director of Audit
4	National Peace and Reconciliation Commission	Leornard Mpofu	Acting Director HR, Admin and Finance
		J.P. Moyo	ICT Manager
		Brain Mangoro	General Manager
5	Zimbabwe Gender Commission	Loveness Batsirai Ndaima	Manager
		Hilary Masenga	ICT Manager
		Sandra Mudzengerere	Public Education and Information Manager
6	Ministry of Environment, Climate and Wildlife	Shimta Nembaware	Complaints Handling and Investigations Manager
7	Ministry of Defence	P Mazhara	Deputy Director, Engineering and ICT
		J. Tandangu	Deputy Director Admin
		R. Tsvangirayi	ICT Officer
8		Lt. Col. S. Chidemo	Staff Officer ICT
		Donald Mhene	Director ICT

No	MDA	Name	Designation
	Ministry of National Housing and Social Amenities	Webster Chidavaenzi	Deputy Director ICT
9	Ministry of ICT, Postal and Courier Services	Newman Ishe Chinofunga	ICT Officer
		I. Njanji	Business Solutions Officer
		R. Maunze	Principal Systems Engineer
10	Ministry of Information, Publicity and Broadcasting Services	Tendai Muyengwa	Information Security Officer
		Zvidzai Masukusa	ICT Manager
11	Ministry of Higher and Tertiary Education, Innovation, Science and Technology Development	Kudzai Manangazira	ICT Officer
		Cephas Ganyele	Director ICT
		Forbes Nyamayaro	Deputy Director ICT
12	Public Service Commission	Bonface Muzvidziwa	ICT Database administrators
		Sandirai Jombe	ICT Manager
		M. Mujuru	ICT Manager
13	Rural Infrastructure Development Agency	B. Dumwa	Systems Administrator
14	Ministry of Youth Empowerment, Development and Vocational Training	G. Makosa	Deputy Director-ICT
		B. Sichewo	ICT Officer
		P. Khumalo	ICT Officer
15	Public Service Labor and Social Welfare	D. Ravasingadi	M&E Officer
		Joe Sherman	Deputy Director - ICT

No	MDA	Name	Designation
		Paungano Amos	A/Deputy Director - Child Protection
16	Zimbabwe Land Commission	Hobwani Samuel	Deputy Director - Economic and Research
		Solomon Tsikai Chinembiri	Manager ICT
		Gibson Mandaza	General Manager Legal Services
17	Ministry of Finance and Investment Promotion	Kelman Taruwinga	General Manager Lands Audit and Inspection
		Tendai J Tazvivinga	Director ICT
		Justice Mashunye	Deputy Director Systems Admin
18	Ministry of Industry and Commerce	Chengetai Gurai	Deputy Director Networks
19	Ministry of Primary and Secondary Education	Muwandi Masibela	Senior Economist
		Chademana Kudakwashe	ICT Officer
		Dhliwayo Ester	Principal ICT Officer
20	Ministry of Foreign Affairs and International Trade	Munwiro Jacob	ICT Officer
		Innocent Vengesai	Deputy Director
		Tafadzwa Masaya	Senior ICT Officer
21	Ministry of Lands, Agriculture Fisheries, Water and Rural Resettlement	Janeth Tavengwa	Deputy Director Administration
		Nyikayaramba Thomas	Deputy Director IT
		Chikobvu Shamiso	Chief Agriculture Specialist (ARDAS)
22		Mugova Agnes	Deputy Director (SPBD)

No	MDA	Name	Designation
	Ministry of Mines and Mining Development	T. Singizi	Director ICT
		S. Kachote	Deputy Director ICT
23	Ministry of Tourism and Hospitality Industry	M.Tagara	ICT Officer
24	Ministry of Transport and Infrastructural Development	Stalyn Chingarande	A/Deputy Director ICT
		Debra Gwazai	Deputy Director ICT
		George Magombeyi	ICT Officer
25	Ministry of Local Government and Public Works	Crezia Chiriya	ICT Officer
		N. Chikugwe	Director, ICT
		T. Machona	Deputy Director
26	Ministry of Health and Child Care	M. Mubhika	ICT Officer
		Trymore Chawurura	Deputy Director
		Linda Maxwell	Software Program Analyst
27	Ministry of Home Affairs and Cultural Heritage	G. Foya	Systems Administrator
		Respect Jongwe	Deputy Director Monitoring and Evaluation
		Shamiso Mutanga	Planning
28	Ministry of Justice, Legal and Parliamentary Affairs	Kudzanai Pamela Chari	Systems Analyst
		Archford Muchengeti	ICT Officer
		Salome Ngandini	ICT Officer
29	Ministry of Sports, Recreation, Arts and Culture	Rufaro Muchirahondo	ICT Officer
		Precious Shonhayi	Recreation Officer

No	MDA	Name	Designation
30	Ministry of Energy and Power Development	Masaka Milton	Arts and Culture Officer
		Silence Chiota	IT Officer
		Melody Msengi	Deputy Director Strategic Policy Planning
31	Ministry of Veterans of the Liberations Struggle Affairs	Patridge Ndemera	Acting Deputy Director Power Development
		Kudakwashe Nyamutumbu	ICT Officer
		Sandra Mabika	Deputy Director
33	Parliament of Zimbabwe	Edzai Marowa	Harare Provincial Field Officer
		Helen Dingani	Deputy Clerk of Parliament
		Nersbert Samu	Chief Director Programs
34	Judicial Service Commission	Teresa Kamvura	Director ICT
		T. Munozogara	Deputy Head IT and Records Management
		T. Shundure	Systems Analyst
35	National Prosecuting Authority	C. Ngwenya	Data Centre Engineer
		Masimba Chirau	ICT Manager
		Blessing Manhai	ICT Infrastructural Development and Maintenance
36	Zimbabwe Anti-Corruption Commission	Michael Mugabe	Chief Public Prosecutor
		Irene Langeveldt	ICT Officer
		Rumbidzai Kabunu	ICT Officer
37		Onias Chiroodza	ICT Officer

No	MDA	Name	Designation
	Zimbabwe Media Commission	Watson Muwezwa	ICT Officer
		Florence Nyekete-Nyanyiwa	HR- Manager
38	Zimbabwe Electoral Commission	T. Shoniwa	Media Training and Development Manager
		Noel Shumba	Acting Director ICT
		Desai Nyamutamba	Systems Administrator
39	Immigration Department	Brian Mhonda	ICT Officer
		PIO Oscar Chitsa	IT Technician
		Mashavakure Tafadzwa David	Principal Immigration Officer
40	Zimbabwe Revenue Authority	Gondo Tigerepayi	Principal Immigration Officer
		Mr. S. Moyo (Project Champion)	Director ICT
		Mr. E. Makunganya (ICT Subject Matter Expert);	Head ICT Security
41	Zimbabwe National Roads Administration	Xavier Matambo (Strategy Expert, Business Processes)	Strategy research and innovation
		Phillip Chingwaro	Head of IT
42	Postal and Telecommunications Regulatory Authority of Zimbabwe	Shadreck Pende	Financial Accountant
		Mr. Alfred Marisa	Deputy Director General
		Dr Richard Munyanyi	Deputy Director –Corporate Services
		Mr. Talent Munyaradzi	Manager – Economics, Tariffs and Competition

No	MDA	Name	Designation
43	Zimbabwe Republic Police	Mrs Mavis Maunganidze	Manager - Universal Service Fund Projects
		Gomo Gajiwett	Chief Superintendent
		Harzel Shambare	Superintendent
44	Registrar General, Civil Registry	Mutevere Havurovi	Inspector
		Nicholas Chimuriwo	Deputy Registrar General, Systems Development & Management
45	Zimbabwe Prisons and Correctional Services	Munei Chiku	Systems Analyst
		Edward Maponga	Director ICT
		E. Zivanai	Staff IT Officer
46	Zimbabwe Electricity Supply Authority	Kudakwashe Mugoniwa	CCO
		Leslie Mukarati	Head IT
		John Chikeya	Commercial Services Manager
		Lucia Sibanda	Thermal Boilers & Turbines Specialist
47	Procurement Regulatory Authority of Zimbabwe	Munyaradzi Mahumucha	Hydro Specialist
		Freddy Ndlovu	ICT Director
		Kilford Jombe	ICT Specialist-Infrastructure & Support
48	Telone	Benson Misi	ICT Specialist-Software Development & Integrations
		Initial Mlambo	A/Technical Director
		Juliet Machiwa	A/Information Systems Head
49	Government Internet Service Provider	Tafara Chipunza	A/Infrastructure Operations Head
		Isaac Munyaradzi	Head
		Nyasha Nyanzunda	Deputy Head GISP
		Zano Mutsindikwa	System Administrator

Delivering a seamless Government experience

D4-2 Integrated Public Service Architecture

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Index of Figures

Index of Tables

Definitions

Term	Definition
Public Service	Provided by the institution to a natural or legal person at his will, including the presumed will through a service contact point in any communication channel and enables the person to fulfil an obligation or exercise a right arising from the law.
Digital Public Service	Provided by the institution to a natural or legal person at his will, including the presumed will through a digital service contact point and enables the person to fulfil an obligation or exercise a right arising from the law.
Integrated Public Service	Result of designing and providing governmental services in such a way that end users can access them through a single seamless experience based on their needs.
Service Owner	Specific person in the ministry or other government institution who is accountable for the service.

Abbreviations

Abbreviation	Description
ABB	Architecture Building Blocks
G2B	Government to Business
IPS	Integrated Public Service
KPI	Key Performance Indicator
MDA	Ministries, Departments and Agencies
NGO	Non-Government Organizations
OPC	Office of the President and Cabinet
SDF	Service Design Framework
SLA	Service Level Agreement

Abbreviation	Description
ToT	Training of Trainers
ZWoGA	Zimbabwean Whole of Government Architecture

1 Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the " An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for enterprise architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves, and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to enterprise architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

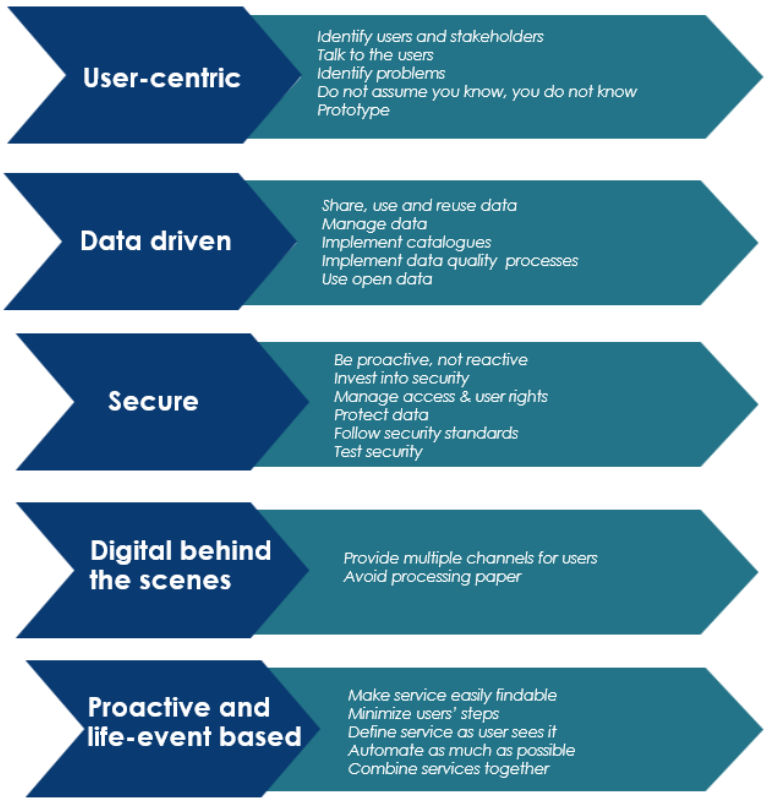


Figure 12 Good practices Integrated Public Service Design.

Public service provision requires that different public administrations work together to meet end users' needs and provide public services in an integrated way. A good public service is integrated with the Government architecture, user-centric, data-driven, secure, digital behind the scenes, proactive and life-event based.

To achieve integration and design user-friendly public services, they must be designed and implemented in a coordinated way. Specifically:

1. ZWoGA must be implemented, and enablers must be used.
2. A systematic, unified, and scalable approach to service design must be implemented, including:

    2.1. Unified framework/methodology for designing, redesigning and development.

    2.2. Knowledge base for different users/actors.

    2.3. Knowledge centre for capacity building and knowledge base management.

    2.4. Tools for design and development.

3. Services need to be based on life or business events and combined.
4. Services need to be easy to find, similar and provided via multiple channels.
5. Knowledge and experience must be shared to learn from success stories and failures.

The IPS Architecture domain is focused on creating a cohesive and unified framework that enables seamless delivery of public service across various MDAs. This domain aims to enhance efficiency and improve the citizen experience while fostering interoperability among different Governmental functions to help the Government of Zimbabwe deliver the expected goal.

Benefits of IPS include:

- Improved service delivery, where citizens can access multiple services through a single interface, reducing the need to navigate different systems and MDAs.
- Increased efficiency, where automation and process optimization reduce manual work and speed up service delivery.
- Enhanced security and compliance, where centralized management of security and privacy ensures compliance with regulations and protects citizen data.
- Cost saving, where streamlined processes and shared infrastructure reduce operational costs for the Government of Zimbabwe.

The IPS layer of the ZWoGA is tightly linked to other architecture layers and foundational projects (enablers). All these dependencies between different domains are described in Chapter 5 of this document.

Implementation of described good practices, building blocks and enablers will help Ministries and other Government institutions provide better services.

The current document is addressed to heads of IT departments, service owners, business analysts, technical architects, and everyone else involved in designing and implementing public services:

1. Public Sector Reforms and Performance Management Department
2. Public officials engaged in the projects of designing and developing digital public services at both executive and administrative levels (e.g., services, Government to business (G2B) services).
3. Public officials are responsible for change management and capacity building.
4. The Ministry of ICT, Postal and Courier Services.

This document describes the architecture of integrated public services, including the Architecture domain [*Chapter 2*], building blocks [*Chapter 3*], organisational view [*Chapter 4*], and dependencies [*Chapter 5*].

2 Architecture Domain

The IPS Architecture includes the following artefacts:

1. IPS Conceptual Model - main concepts related to development, management and provision of integrated public services.
2. List of methodologies to implement IPS: These can be guidelines, recommendations, and a common set of requirements for designing, redesigning, and developing.
3. List of tools that provide working mechanisms that assist MDAs to implement IPS. Tools can be the following: public service design service mapping, description, visualization, monitoring, assessment, project preparation.
4. List of relevant trainings. As it is expected that specific skills must be popularised among MDAs this artefact will look to propose necessary training aspects: materials and environment for the MDAs (e-learning platform) supported by a knowledge base, training of trainer (ToT) and capacity-building programs.

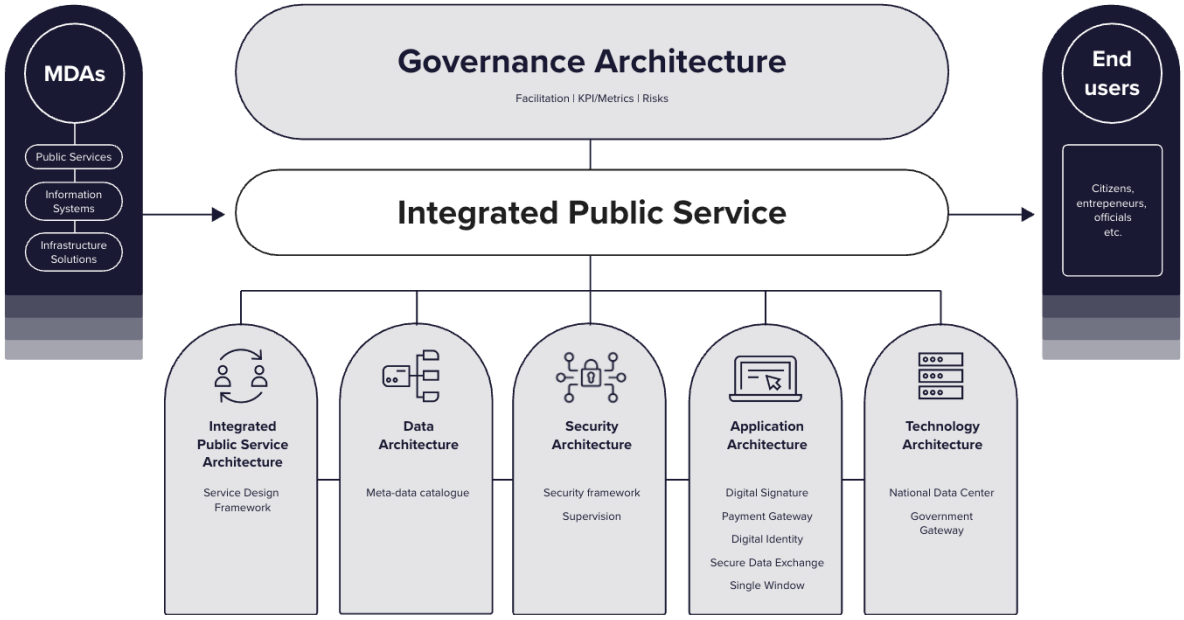


Figure 13 Zimbabwe Whole of Government Architecture

2.1 IPS Conceptual Model

Traditional Public Service from a remarkably high abstraction level and simplification can be presented as the exchange of information and resources between the end-user (User) and the service provider (Public Service provider). As it is common that one entity provides multiple public services, then it is reasonable to separate the public service from its provider as a separate concept.

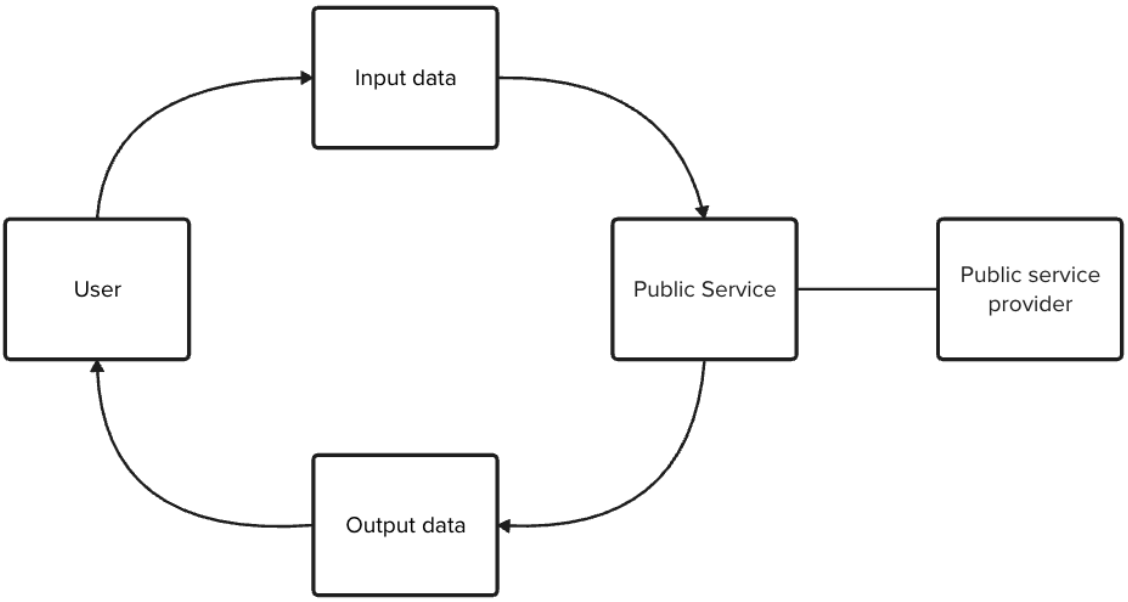


Figure 14 As-Is Public Service

If the public service provider works independently, the potential of optimization is limited to the same entities' resources and information provided by the public service user. Therefore, from the Whole of Government's perspective, it is a desirable situation that public service providers would cooperate when providing public services. This approach and concept can be defined as:

Integrated public service is a public service provided by the public service provider in cooperation with other public service providers to recognize the wants and needs of the service user.

This approach must be understood with the following aspects in mind:

- For citizens and entrepreneurs (users), public services are relevant and needed when an event happens, a need is identified or the environment changes. It cannot be expected that in those situations, the needs of the user match one-on-one to exactly one public service. Therefore, a need from the user is usually related to multiple public services.
- Recognizing the relationships between user needs and different public services we expect public service providers to cooperate.
- For an integrated public service, information output by one service provider can and often is the input for other service providers. Information alone is

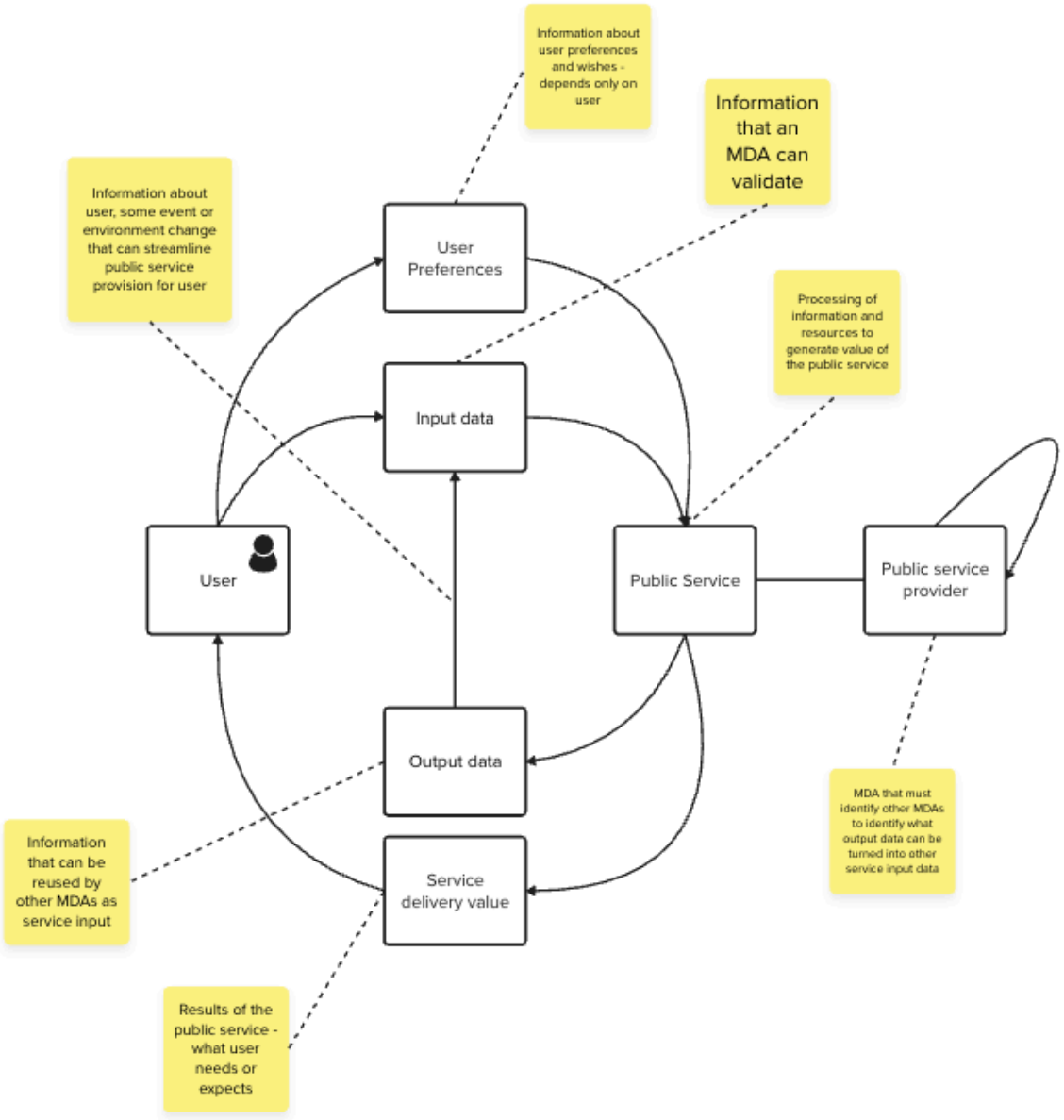


Figure 15 Integrated Public Service Conceptual Model

usually not relevant or expected result for the user - the user expects the value of the public service to be delivered.

- Reacting to the need and change and moving between public services, the user should have the opportunity to submit its preferences and expectations related to the public service.

These aspects allow us to sketch the Zimbabwean conceptual model of integrated public service.

2.2 List of methodologies

The following artefact presents a list of methodologies and their relevance in current and future iterations of the WoGA.

Table 14 Artefact: List of methodologies

Methodology	Short Description of Impact	Target iteration
Service Design Methodology	Instructs MDAs how to (re)-design public services while recognizing capabilities and services from other MDAs and (re)using the data.	1, current
Service Management Methodology	Defines how sustainability of a public service operation must be addressed, defined and monitored.	2, next
Service Monitoring Methodology	Provides common approach for measuring the quality of a public service.	3, future
Data Management Methodology	Commonly agreed approach how data is collected, stored, described and how data quality is managed (related to Data Architecture)	2, next

2.3 List of Tools

The following Artefact presents tools for adopting ZWoGA and IPS from the IPS Architecture level - tools for the service owner. As individual tools can be small snippets, then at the ZWoGA level it is relevant to expose toolboxes - a collection of similar tools that stakeholders can use when following methodologies enforced by the ZWoGA.

Table 15 Artefact: List of toolboxes

Toolboxes	Description of toolbox	Target iteration
Service Design Tools	Tools helping service owner and service designer to create	1, current
Service Quality Tools	Tools to measure service quality from various users and various perspectives.	2, next
Service Management Tools	Tools helping to manage service provision and development from organisational and financial perspective.	2, next

2.4 List of Training

This Artefact contains and aggregates requirements of training driven by the IPS approach. The pieces of training consolidated here are relevant to ensure that a skill-building mechanism would exist for MDAs to nourish the ongoing development of public services when respecting the IPS approach. The Learning Programme for Public Service Design and Reengineering is described in chapter 9.10 of the Change Management Strategy.

Table 16 Artefact: List of training

Training	Description of training	Target iteration
Service Design	Enhancing skills related to service (re-)design.	1, current
Service Ownership	Enhancing skills related to covering whole service lifecycle.	2, next

2.5 Beneficiaries of IPS Architecture

The IPS Architecture domain in Zimbabwe serves a wide range of beneficiaries and users. By creating seamless, efficient, and integrated public services, with a user-centric service delivery model, this architecture domain aims to enhance the overall experience of government services to ensure they meet the demands of all involved stakeholders. The beneficiaries of this architecture domain can be categorized into several groups based on their interaction with government services and their roles within the public service ecosystem.

The primary beneficiaries and users include:

- **Citizens:** individuals who need to access multiple government services through a single integrated platform.
- **Businesses and service providers:** private sector entities that interact with Government agencies for various regulatory, licensing, and support services, and Non-Governmental Organisations (NGOs) that provide services or support to the Government. The role addressed by IPS Architecture is "Service Owner".
- **Government employees:** public sector employees who are responsible for delivering, managing, and supporting Government services - service owners.
- **MDAs:** various Governmental bodies responsible for providing services, enforcing regulations, and supporting public welfare with seamless integration and shared data across different departments.

- **Policymakers and Regulators:** bodies or individuals involved in the formulation of policies, laws, and regulations, they need access to comprehensive data and analytics to inform policy decisions and have a better assessment of policy impact and outcomes.
- **Researchers and Academics:** institutions and individuals engaged in research and academic studies related to public administration and services, to get access to comprehensive integrated data sets for research.

3 Architecture Building Blocks

IPS Architecture defines the following building blocks:

- **Roles:**
  - **Service owner** - a specific person in the MDA who is accountable for the quality of service. The service owner is not acting alone; he/she needs to be supported by the management with sufficient resources. He/she is the principal recipient of IPS architecture. Core responsibilities involve specifically:
    - Service development and implementation of business processes.
    - Service operation and governance.
    - Service improvement.
    - Service assessment.
    - Communication with stakeholders.
    - Service financing.
    - Service support.
    - Risk management and mitigation.
  - **Service Design Task Force** - a focal role conducted by a small team from OPC to ensure the IPC Architecture domain is implemented.
- **Environments:**
  - Knowledge Base - a centralised body repository for storing and easy access to methodologies and toolboxes.

- **Training environment** - dedicated learning platform to help the Service Design Task Force deliver training related to Integrated Public Services Architecture. It is expected to be implemented in cooperation with the Public Service Commission.

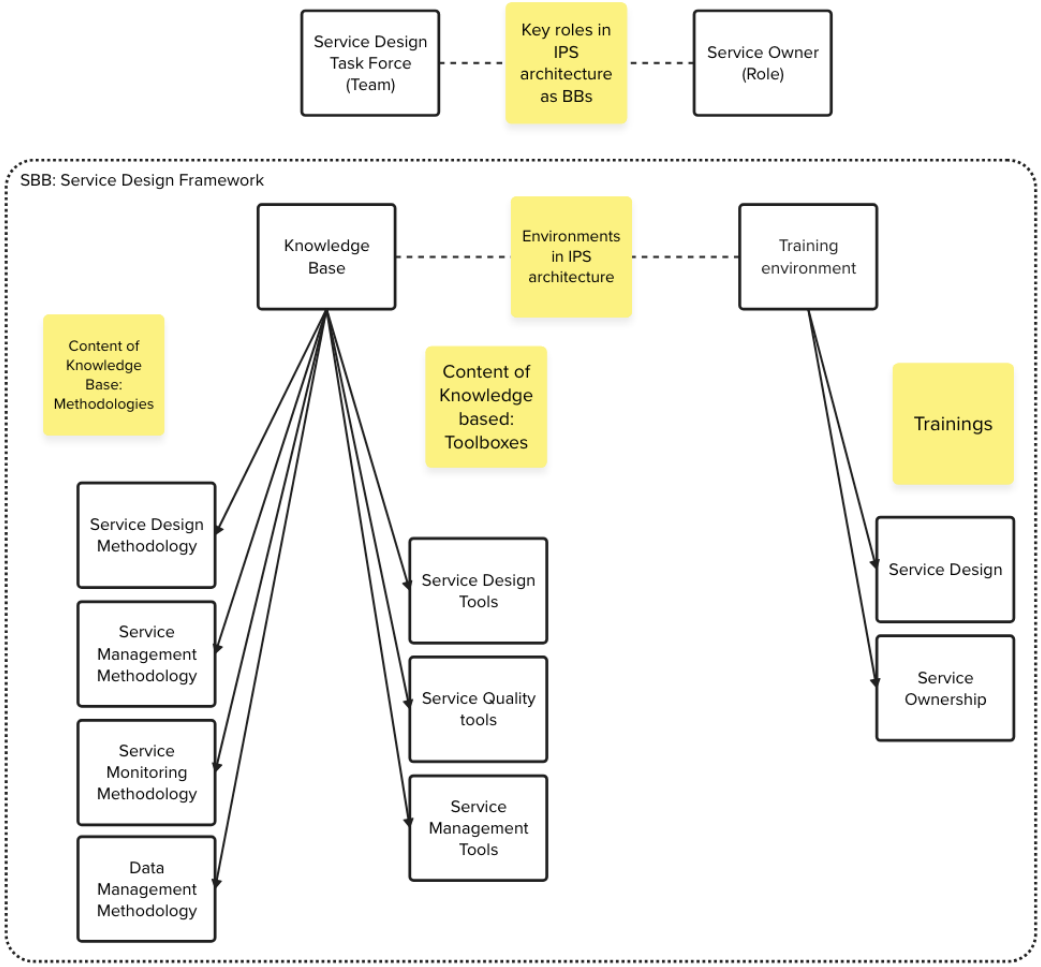


Figure 16 IPC building blocks.

For smooth delivery and effective implementation, the content elements for the Knowledge Base and Training environment (with the initial establishment of the environments) are implemented as one solution building block - The Service Design Framework (SDF). This will provide the necessary methodology, tools and training materials for the MDAs, supporting them in digitalising their services and data. SDF creates a common ground and requirements for MDAs in designing digital public services in Zimbabwe.

The specific content of each building block will be described and developed during the foundational project. Necessary steps in implementing SDF:

1) Development of SDF:
   a) Development of service design methodology.
   b) Description of the tools supporting MDAs in methodology implementation.
   c) Development of training materials and e-learning platform.
2) Conducting pieces of training for service owners and supporting their first digitalisation projects.
3) Conducting a pilot service digitalisation. The first service to be digitalised and redesigned as IPS is the registration of birth/issuance of birth certificate because it:
   a) Concerns most of the population.
   b) Enables to eliminate data duplication, data can be used by many MDAs, and it is possible to start collecting the following information in digital form: full names, addresses, gender, date of birth, and entry number/identity.
   c) This is related to a big workload - more than 100 applications are submitted per registration office per day.
   d) Enables to speed up back-office procedures.
   e) Is easy to develop, and the necessary infrastructure is in place.

The registration would include full names, addresses, gender, and date of birth/birth entry.

3.1. Knowledge base

The Knowledge base serves as a central repository for methodologies and toolset descriptions, templates and other essential resources. It facilitates easy access to critical information that can aid in the efficient execution of tasks and projects. The knowledge base should be continuously updated to reflect the latest methodologies, toolset updates and newly developed templates, and all team members are encouraged to contribute to the knowledge base by sharing their insights, experiences, and improvements to the existing content.

The knowledge base includes:

- A detailed description and guidance on various methodologies employed within ZWoGA to provide step-by-step instructions, and key considerations to ensure consistent application across different teams and projects.
- A comprehensive information about the tools and technologies used within ZWoGA, to help the team members and MDAs select and utilize the appropriate tools for their needs.
- A collection of standardized templates for distinct types of documents and deliverables, including, project plans, reports, presentation slides, and all other commonly used documents.

3.2. Service Design Methodology

The most critical methodology for establishing IPS is the Service Design Methodology. This must be established as one of the early/foundational core elements to kick-start the creation of integrated public services.

The Methodology must include guidelines, recommendations, and a common set of requirements for designing, redesigning, and developing digital public services. Specifically:

1. Service design principles.
2. Description of the service design process.
3. Recommendations and examples of how to identify and describe user needs.
4. Overview of existing guidelines, legislation, and recommendations.
5. Description of user-research methodologies.
6. Description of the service development process.
7. Description of the minimum skills of MDA teams responsible for integrated public service development and management.
8. Description of the data digitalisation principles.
9. Description of the data management principles.

3.3. Service Design Toolbox

Tools for public service design will support MDAs in service mapping, describing, visualizing, testing, monitoring, and assessing. Specifically:

1. Description of the necessary steps for designing integrated public services through the service lifecycle.
2. Description of the needed activities for service mapping and suggesting proper tools for such activities together with user guides for such tools.
3. Description of how business processes and use cases (AS-IS and TO-BE) should be described and suggest suitable tools together with user guides.
4. Description of how business requirements should be described and managed and suggest suitable tools together with user guides.
5. Description of the methods and tools for user research.
6. Description of the methods and tools for user testing.
7. Description of the prototyping process along with a suggestion of proper prototyping tools.
8. Development or suggestion of tools for effective performance management to monitor and assess the performance of public services.
9. Description of how to measure service quality and user satisfaction (incl. dev of KPIs).
10. Development of example Service Level Agreements (SLAs).

3.4. Training Environment

The training environment is an online platform designed for the creation and execution of training programs within the IPS Architecture domain. It is primarily focused on providing comprehensive training resources for service owners to enhance their understanding and capabilities within the IPS Architecture domain to be able to contribute to more efficient and effective service delivery. Key features and benefits of this training environment may include, designing training programs, executing training, comprehensive curriculum, engaging and interactive content, collaboration support, and progress tracking and reporting.

3.5. Service Design Training

Training materials will be part of the online knowledge base, together with the online training environment and related materials supported by ToT programs aimed at training the task force. Specifically:

1. Development of a technical solution for the knowledge base and learning environment.
2. Development of a comprehensive plan for capacity building.
3. Delivering training, consultations, mentoring, and other capacity-building programs for task force members.
4. Provision of training, consultations, mentoring, and other capacity-building programs for the learning environment administrators to independently maintain and manage the training environment.
5. Implementation of the ToT approach to assemble a proficient team supporting MDAs in the adoption process.
6. Development of an e-learning platform and creation of online courses for MDA officials about public service design and development.
7. Development of online courses with self-assessment tests and feedback forms for trainees.

4 Organisational view

IPS is owned and its implementation is managed by the e-Government Technology Unit under OPC. Capacity-building activities like the development of online courses are done in cooperation with the Public Service Commission.

The e-Government Technology Unit will support MDAs during the design and development of integrated public services by creating a related methodology, making available necessary tools, and learning environment together with the knowledge base.

Implementation support by the unit means:

1. Conduct different capacity-building programs.
2. Conduct ToT programs.
3. Empower the task force that supports MDAs during their first service design projects.

MDAs are expected to:

1. Adjust their internal work processes in such a way that implementation of ZWoGA, especially the development of IPSs together with SDF is supported.
2. Assign specific people responsible for implementing SDF.
3. Allocated sufficient funds needed for service design.
4. Support and participate in capacity-building programs.
5. Participate in different working groups, sharing knowledge (both success stories and failures), and giving feedback to the SDF.

5 Dependencies

All domains and components of the ZWoGA (see Figure 13) are linked and developed to support the whole digital Government ecosystem.

Additionally, the building blocks of different domains and enablers (foundational projects) are tightly linked to IPS, as described below:

1. **Data Architecture:**
    a. Designing IPS relies heavily on digital data, meaning that information about collected data, is needed when designing or redesigning public services.
    b. Data can be used or reused if it is in digital format. Data Architecture establishes principles and good practices for how digital data should be stored, described and shared.
2. **Application Architecture:**
    a. **Data exchange.** User-friendly services can only be provided if data is shared and reused (once only principle). Data sharing relies on the quality of the data and a secure data exchange platform. Application Architecture defines the needed principles, good practices, standards, and procedures.
    b. **Digital Identity**. When providing services, it is important to know who is behind the screen or who is using the mobile phone to apply. Application Architecture creates rules and requirements for secure authentication and digital signing, so these components can be integrated into digital services.
    c. **Single Window.** Public services must be easily accessible and found, meaning that they are provided using a single window. Such an approach must be considered during service design.
    d. **Payment Gateway.** Payment for the services needs to be easy and fast, meaning that the Payment Gateway solution must be integrated into the public services enabling both fast payment and its checking.
3. **Security Architecture:**
    a. Digital services can only be trusted if they are developed using secure solutions and tools. Therefore, while designing integrated public services, cross-functional requirements need to be considered. On the other hand, security architecture must be flexible enough so user-friendly services can be provided.
4. **Technology Architecture:**
    a. When designing new services, requirements for the technology and an agreed approach to the technical solution must be considered.

b. Technology Architecture, on the other hand, must consider with needs and expectations of service design to provide the best services to the end users.

5. Joint components of each domain:

a. **Legal framework.** Mandatory use of digital identity, acceptance of digital signatures, the option to share data and other foundational components need to have a legal basis.

b. **Financing.** A clear agreement on how the development and management of public services are financed is part of the ZWoGA.

Delivering a seamless Government experience

D4-3 Application Architecture

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Table of Figures

Index of Tables

1 Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the "An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean Vision for Enterprise Architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to enterprise architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

Application Architecture provides a blueprint for the Zimbabwean Whole of Government Architecture (ZWoGA) individual platforms to be deployed.

Platforms – techno-organizational solutions that provide some common digital infrastructure to the MDAs – and their interactions with information systems that provide core public services and processes of the government.

Application Architecture is built upon the architecture of integrated public services – defining the environment of platforms into which the information systems of the MDAs are constructed and situated. The platforms defined in Application Architecture reduce the number of functionalities that must be implemented into the information systems of MDAs. The platforms will provide new possibilities to enrich the information systems of the MDAs, and the public services provided by the MDAs. Tighter integration among MDAs using platforms helps to reuse capabilities and avoids recurring costs – additionally, the development of new services is accelerated.

2 Application Architecture Domain

The objectives of the Application Architecture are to:

- Understand the current situation as the baseline.
- Develop the Target Application Architecture that enables the Business Architecture and the Architecture Vision, in a way that addresses the Statement of Architecture Work and stakeholder concerns.
- Identify candidate Architecture Roadmap components based on gaps between the Baseline and Target Application Architectures.

Application domain-specific view contains the most salient Application Architecture Building Blocks that need to be considered to support technical aspects for the end-to-end design of the applications essential for Integrated Public Services.

ZWoGA Application Architecture defines Foundational Enablers to be used by MDAs when (re)designing their business processes.

2.1 Artefact: Common Functional Requirements

The Integrated Public Service (IPS) Architecture exposed that the approach to how public services should be provided must be defined by a common methodology. From

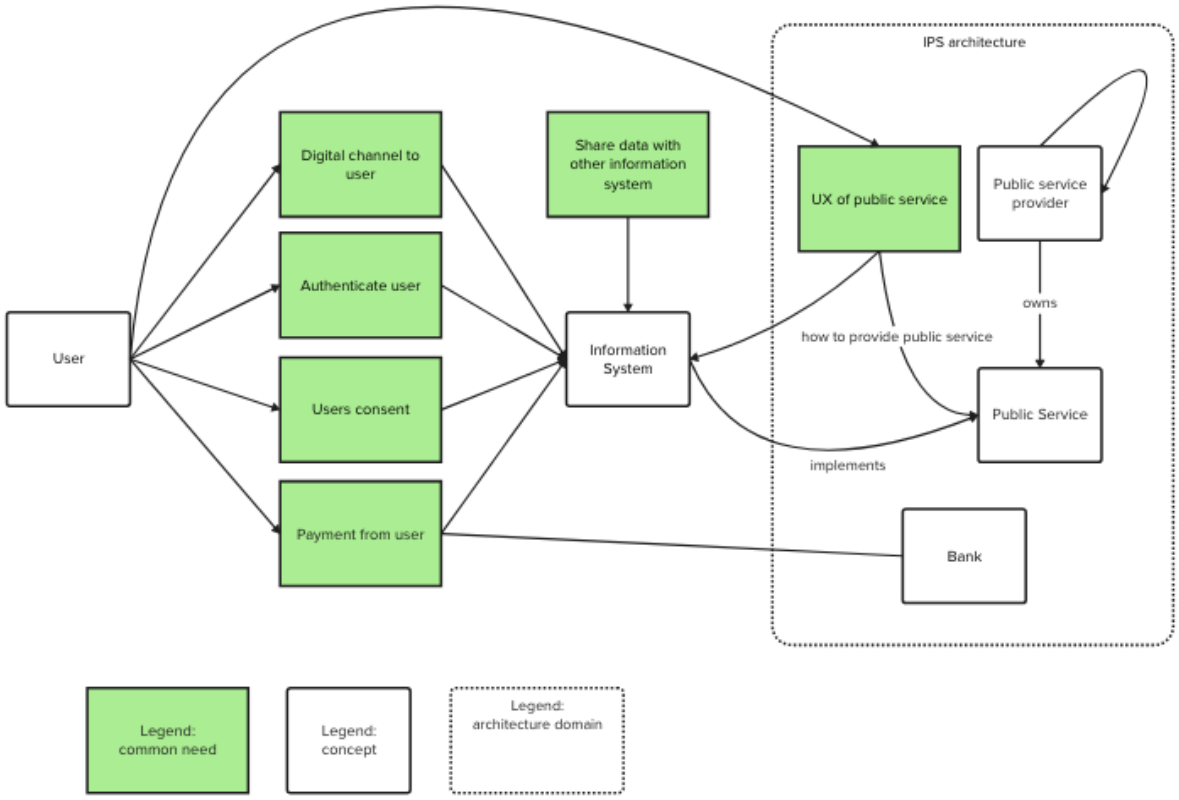


Figure 17 Common Functional Requirements

the end-user perspective "how a service is received" is commonly addressed as user experience (UX). The IPS Architecture also defined that cooperation between public service providers is needed to make public service better for users. At the application architecture level, it must be defined that public service (data processed, necessary procedures and proceeding) is implemented using an information system by an MDA. An information system is a set of technical (software and hardware) and organisational resources that are used in a specific way to deliver public service. By using ICT as a technical resource, it has been identified by the MDAs of Zimbabwe that a known set of common needs exist that should be addressed by a common approach. The needs that have been identified are:

- **Share data with other information systems** – send and/or receive information based on regulations and contracts between MDAs/public service owners and their information systems.
- **Digital channel to user** – reaches out to end-users in the digital environment.

- **Authenticate user** – ensuring that the identity of the user accessing the public service through the digital channel is certain at the necessary level of security and assurance.
- **Consent user** – ensuring that the end-user gives its full consent on an application, decision or any other data set.
- **Payment from user** – ensure that when using a public service in a digital channel and there is a need for fee payment, it can be executed without leaving the digital channel.

The common needs described above and sketched in Figure 17 were identified because of the first iteration of workshops held in Zimbabwe in April 2024. Those also constitute the most urgent needs that are relevant in the application architecture context (infrastructure-related needs are exposed in Technology Architecture).

2.2 Artefact: Platform Portfolio

The table below identifies the initial version of platforms in the Application Architecture domain.

Table 17 Platform Portfolio

Platform name	Principal owner	Architectural choices	Candidate solutions
Data Exchange	OPC	(Micro-) Service approach for MDAs. Small skillset for DevOps, developers and Administrators/ Maintainers. No transformation of data to preserve integrity.	X-Road by NIIS.
Digital Identity	Civil Registry Department	Provide Government-issued Digital Identity. Additionally address both: Authentication Services Gateway (for Government and other Authentication Services) and SSO.	
Digital Signature	OPC	Container based format with verifiable Digital Signature. Legally binding and equal to hand-written signature.	XAdES, ASiC-E

Platform name	Principal owner	Architectural choices	Candidate solutions
Single Window	OPC	Platform supports MDAs to have similar end-user look and feel. UX responsibility on MDAs. Following Micro-Frontend (MFE) and API-First Principles will help to develop flexible solutions.	
Payment Gateway	OPC	Design and operation in cooperation with banking sector. Use Digital Identity Platform as one of authentication options.	

2.3 Artefact: Interface Catalogue

The following artefact lists the most important interfaces that are architecturally solid. This must be seen as a high-level requirement when building/implementing/procuring the platform.

Table 18 Interface Catalogue

Platform	Interface	Key functionality	Design principles
Data Exchange	Security Baseline and PKI	Ensures Encryption (mutual) and Integrity using common services from PKI.	Recommended Standards: CSR, OCSP, RFC3161, TLS.
Data Exchange	Discovery	Provide discoverability inside the platform.	RESTful, OpenAPI
Data Exchange	Exposure of Data	Expect minimal skills from API designers.	RESTful, OpenAPI
Digital Identity	Certificate Validation.	Real time Certificate status.	Recommended Standards: OCSP.

Platform	Interface	Key functionality	Design principles
Digital Signature	Certificate Validation	Real Time Certificate status.	Recommended Standards: OCSP.
Digital Signature	Timestamp	Time evidence for signature	TSA, NTP, RFC3161

2.4 Artefact: Application-Platform Interaction Model

The introduction of the IPS approach and the launch of platforms to assist MDAs in providing public services is a major change for many stakeholders. The first iteration of Application Architecture recommends a set of platforms to help MDAs create effective integrated public services.

The Target Architecture can be described: platforms help MDAs and their information systems to reduce the technical skill and resources from interactions and allow the MDA to focus on improving their systems to be ready for integrated public service and cooperating with other MDAs:

- **G2G** – a data exchange platform to make information available and possible to exchange between MDAs.
- **G2C/G2B** – a set of platforms (digital identity, single window) to reduce the technical complexity of reaching out to the end-user (citizen or entrepreneur).

The generalized flow of interaction is drafted in Figure 18.

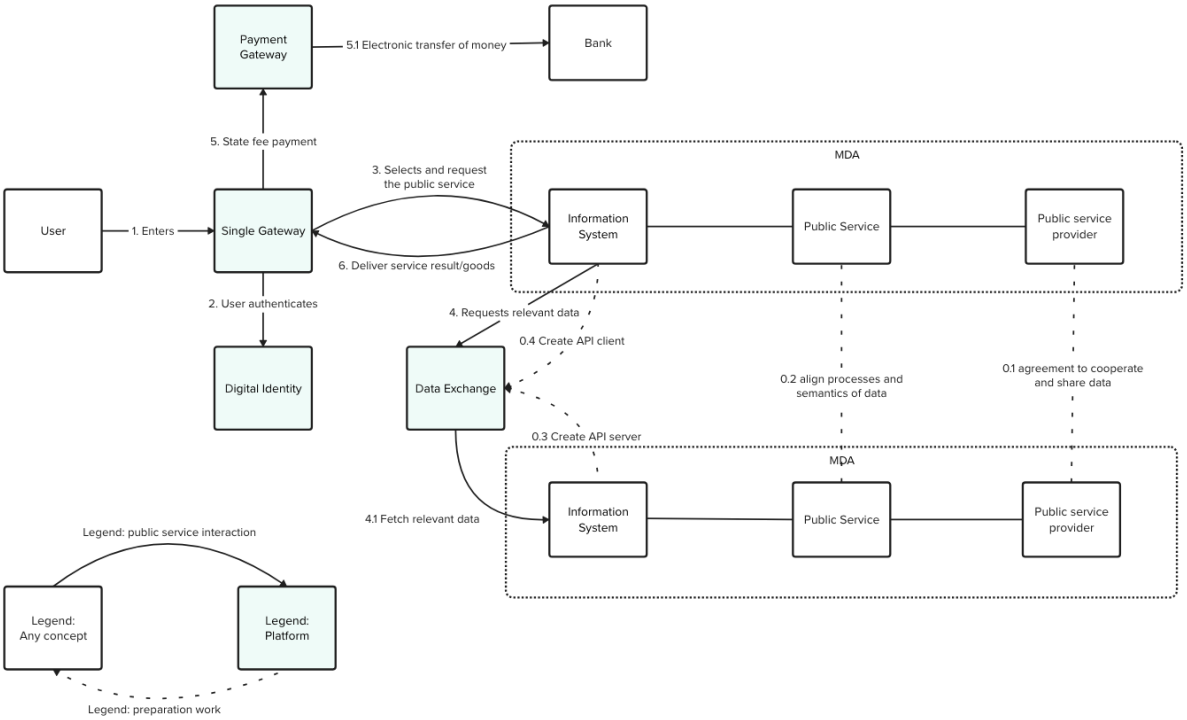


Figure 18 Application-platform Interaction Model

3 Architecture Building Blocks

The most important building blocks of Application Architecture are described below because of application architecture work. The description of building blocks comes from two sources:

1. Discussions and exercises conducted by MDAs in Architecture workshops.
2. The consultant described best practices from the world that are aligned with positions in Zimbabwe.

An overview of what needs are addressed by specific platforms is presented in Figure 19. In future iterations when the need becomes more specific it is expected that the relationship between needs and platforms can be **n:m** relationship as platforms will start to consolidate needs related to similar topics.

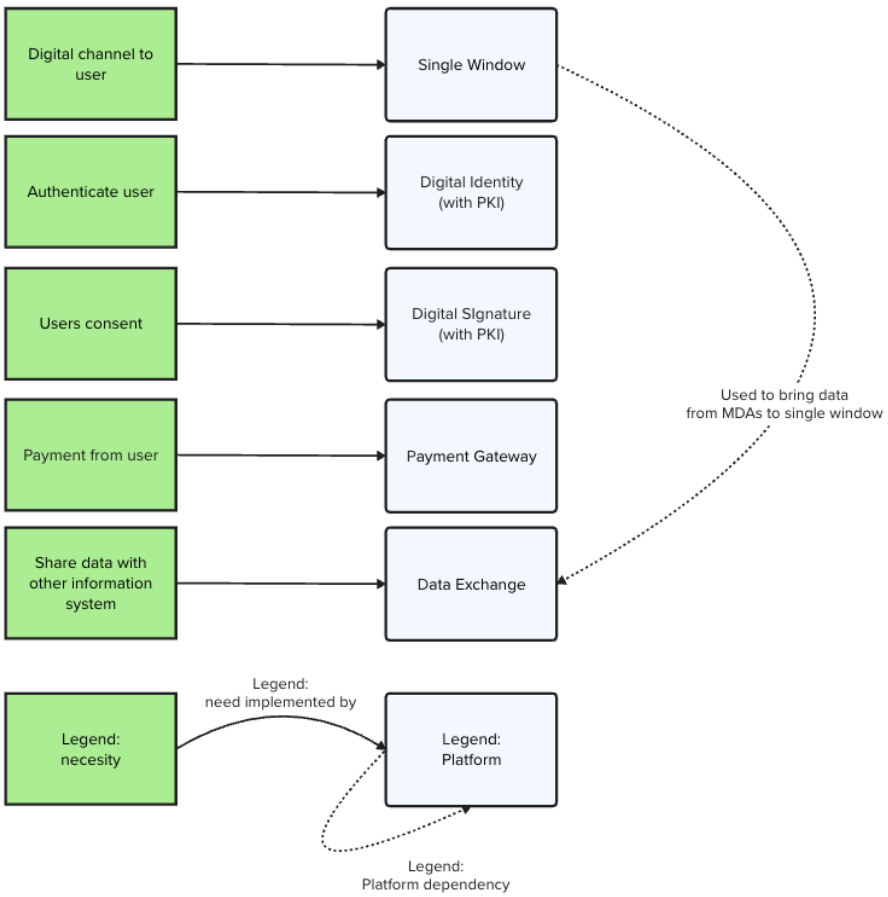


Figure 19 Need to Platform Relationship

3.1 Data Exchange

Key requirements for data exchange:

- Relay on existing network connectivity and use public internet as baseline connectivity.
- Access control to information controlled by MDAs.
- Data access through APIs that are defined and created under MDA control. Access control must support at least an API-endpoint-to-consuming-MDA level of access. The access control mechanism provided by the Platform can be more detailed.
- Centrally managed MDA participation in the platform. Also, open to the private sector.
- The Platform must ensure the exchange of information that would not reduce its confidentiality.
- The Platform must ensure the exchange of information that would preserve its integrity and give a basis to use exchanged data for automated decision-making (digital signatures or seal or similar mechanism to ensure later verifiability of exchanged data).
- The Platform must support and assist MDAs in using the platform.
- The Platform must provide internal mechanisms for discovery – participating entities (MDAs or private sector) and their services.

3.2 Digital Identity

Key requirements for digital identity platform:

- Based on physical identity and verified by Government authorities.
- Use one universal identifier for a citizen that is linked to the Digital Identity. The identifier must be public, persistent and unique.
- The platform must provide a token for authenticating in various environments:
  - Physical
  - Off-line
  - Online
- Tools for integrators.

3.3 Single Window

Key requirements for the single window:

- The medium/channel for citizens to access digital services must be defined by analysing technical capabilities in society. The channel could be a Web Portal, Mobile App, Hotline, USSD application, … or a combination of those.

- The solutions must be ready to switch from channel to channel. For that, the "API-first" and "Micro-frontend" principles must be adopted by MDAs.
- A unified approach to access services and how services are presented (UX).
- Back-end integration of MDAs using the Data Exchange Platform for as much as possible.
- The User Interface of the Web Application must be accessible. WCAG 2.2 Level AA requirements must be met.
- Multilanguage support with translations to local languages where applicable.

3.4 Digital Signature

Key requirements for digital signature:

- Cryptographical consent for digital content – agreement, payment, image, video, etc.
- A signing Certificate is issued to the subjects that are identified using the Digital Identity Platform.
- Expected container-based format to have readiness for various usage scenarios.
- Acceptable usage scenarios in C2G, G2G, B2B, C2B, B2G... all combinations.

3.5 Payment Gateway

Requirements to be refined at the next Architecture iteration.

4 Organisational view

Without interagency-level intervention, systems do not become interoperable, and it is impossible to develop secure applications or information systems that would allow the creation of integrated public services.

To enable interoperability, technical requirements, standards, baseline solutions and tools must be implemented by a central competent authority. These artefacts must then be introduced to all existing and new projects to enable string interoperability between solutions.

The Governance refers to decisions on implementing foundational enablers of Application Architecture Building Blocks. It includes institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability at the national level. Governance is the key to a holistic approach to Integrated Public Services, as it brings together all the instruments needed to apply it.

5 Dependencies

Application Architecture has the following dependencies on other architecture domains:

- **IPS Architecture** – value provision from platforms must be well known to methodologies and tools used in IPS Architecture as this way it is easier for MDAs to design their integrated Public Services to use the capabilities provided by Application Architecture.
- **Technology Architecture** – Application Architecture Platform must simplify the relationship between MDAs and infrastructure provision. Therefore, any changes planned for Application Architecture Platforms must be negotiated with Technology Architecture service providers as the platform relies on the service from the technology stack.
- **Data Architecture** – Data Architecture is the baseline for MDAs to discover what capabilities can be re-used and cooperation made with other MDAs. These cooperation aspects can be implemented using platforms from application architecture. It is reasonable to integrate the management processes of platforms into Data Architecture data gathering processes as this allows to catch the most critical meta-information changes from the ZWoGA.
- **Security Architecture** – platforms defined in Application Architecture must follow the requirements of Security Architecture just as any information systems from MDA.
- **Governance Architecture** – Application Architecture supports the adoption of the most critical digitalisation aspects and therefore fastens the whole architecture implementation process for MDAs. This defines a two-way relationship between application and governance architecture. While enablers defined in Application Architecture help MDAs to be compliant with a large set of principles then the platforms require governing architecture to support and force the uptake of the platform from application architecture.

Delivering a seamless Government experience

D4-4 Technology Architecture

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Index of Figures

Index of Tables

1 Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the " An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for Enterprise Architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to enterprise architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

Technology Architecture is structuring the services related to commodity ICT services. While other architecture domains are introducing a lot of new capabilities and working practices, Technology Architecture is about building a solid baseline and clear ownership for the foundational layer of architecture. As this is in practice the domains where the most significant results are already available then the focus in the Architecture is to identify clear owners for the building block in this layer.

2 Technology Architecture Domain

The Zimbabwean Whole of Government Architecture (ZWoGA) is looking for an ICT-empowered approach that would prescribe a path for reaching the vision identified by the stakeholders. As the architecture has been split into several domains, the technology architecture represents the technical baseline for all the requirements and expectations. This does not cover just the physical infrastructure and broadband networking but also commodity services expected and needed by the Zimbabwean public sector.

The first iteration of Technology Architecture does not strictly follow the recommended methodology as it will define the initial technical landscape and building blocks. In future iterations, it is expected that there will be refinements about "how" the building blocks of technology architecture are constructed and implemented for users and less about defining new building blocks. The changes that need to be adopted can come from the evolution of technology and best practices of its management but also from alternative cooperation methods with the private sector. As Zimbabwe is big by land area, population, entities in the public sector are very dispersed across the whole country, therefore collaboration with the private sector must be seen as a viable part of Technology Architecture. As such, being able to deliver technically viable services to MDAs and platforms described in other architecture domains remains critical.

Also, in the first iteration of architecture work the emerging technologies steps are left out as the focus is on establishing a solid ownership and structure for all architecture domains. As each emerging technology creates a disruption in the landscape the stakeholders engaged in the architecture work should be critical of emerging technologies.

3 Technology artefacts

The situation analysis and preparation for the first iteration of architecture work exposed a challenging situation in Zimbabwe in the domains that are affected by the technology architecture. The considerations of how the existing situation has been combined into technology architecture are provided in this background chapter.

3.1 Infrastructure

The National Data Centre (NDC) is operational and has significant plans for strengthening its services (multi-location, recovery site etc). However, there are various issues related to its usage. The most important aspect revealed by MDAs is reliability for mission-critical solutions. As a result of ZWoGA implementation it is expected that MDAs will locate their solutions for public service provision into NDC and therefore reasonable infrastructure services options must be available. This requires reviewing the national data centre service offering, its quality and the SLA available.

The current approach has steered MDAs towards using NDC from MICTPCS. While the Ministry of Higher and Tertiary Education, Innovation, Science and Technology Development is expected to pool its high-computing-power resources with the NDC in the future, the NDC is presented strictly as built from governmental resources. However, this policy should be revised and restated – it is expected that for special circumstances usage of other clouds (Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, etc.) should be tolerable and combined use of governmental and private cloud service providers within the country. As shown by other countries limiting one's resources only to what is available in the public sector becomes extremely inefficient in terms of total cost and efficient operation. This calls also for defining a Data Security Policy on using the other cloud services for government services.

3.2 Networking

GISP and NDC both claim that they are responsible for providing connectivity for MDAs. While the situation could not be better for MDAs – there are alternatives for service providers – the MDA reaction is most critical for broadband network services – the availability and bandwidth. These efforts must be joined to provide the best service to MDAs and procuring connectivity from the private sector should be also acceptable. The discussion in architecture work exposed the expectation that there should be one government network service provider while the physical service can be implemented by various providers. The network service must be revised, its true maintenance and operation cost estimated (besides regular wear and tear vandalism and other similar aspects must be considered), and necessary resources acquired. In the resource deficit, it might be reasonable to revise how networking service is provided, and the public-private-partnership approach is assessed.

This calls also for defining a data security policy on using private networking for government services.

3.3 Commodity Solutions

GISP provides e-mail, calendar and other office collaboration services (document management system, employee resource planning etc.). However, there is minimal usage of those services – mostly due to the issues related to availability issues. MDAs are adjusted working in the current situation where various e-mail service providers are used.

The practice comes from several aspects but one most relevant for Zimbabwe should be Cybersecurity – allowing various services from random service providers (most of them foreign to Zimbabwe) poses a security issue as Government information is processed out-of-country and poorly managed domain usage simplifies socially engineered attacks. Every Government employee registering and setting up personal accounts with questionable security settings and using these accounts for Government work – this is a scenario that will not ensure secure and sustainable operation. This requires strict policies on using Government-provided collaboration tools (e-mail, calendar) and other commodity services (document management etc.) and appropriate services to be established by respective service providers. Relevant services have been listed in the technology services matrix.

3.4 Artefact: Technology Policies Catalogue

As a result of Technology Architecture work policies on the following topics are needed and must be defined as part of architecture implementation work.

Table 19 Technology Policies Catalogue

Topic	Key problem	Owner	Adoption date	Status	URL
Public Cloud Usage	Define conditions when MDA can use cloud services from private sector.	OPC	Not adopted	Draft	
Private Networking Usage	Conditions when MDA can use private sector networking services	OPC?	Not adopted	Draft	

Topic	Key problem	Owner	Adoption date	Status	URL
Government e-mail usage	Suggest acceptable e-mail service providers for public sector (also a security concern)	OPC	Not adopted	Draft	

3.5 Artefact: Technology Services and Owners Matrix

Table 20 Technology Services and Owners Matrix

Service	Owner	Description
Infrastructure Hosting	MICTPCS/NDC	Accommodating MDA infrastructure in NDC premises.
Virtual Machine Hosting	MICTPCS/NDC	NDC owns the infrastructure and as a service provides computational power and storage. Service provided in cooperation with Ministry of Higher and Tertiary Education, Innovation, Science and Technology Development.
Website Hosting	GISP	SaaS for MDAs built on top of Virtual Machine Hosting by NDC.
Office Broadband Connectivity	GISP	Provided as cooperation between GISP and NDC.
E-Mail & Calendar Service	GISP	Providing collaboration and productivity tools using SaaS model.
Document & Information Management	GISP	Hosting of document and information management solution for MDAs.

3.6 Artefact: Emerging Technologies Matrix

The challenge with emerging technologies is that at the beginning of the Gartner hype curve and mostly in the "Peak of inflated expectations" an emerging technology steals a lot of attention – many stakeholders want to use and sell it for any use-case. Critical thinking must help those who are responsible for the bigger picture to see long-term impact and balance with existing (also legacy) solutions and approaches. Although for some emerging technologies there is a lot of buzz going on it must be recognized that techno-organisational problems that have been solved (with mature technologies) do not need fixing.

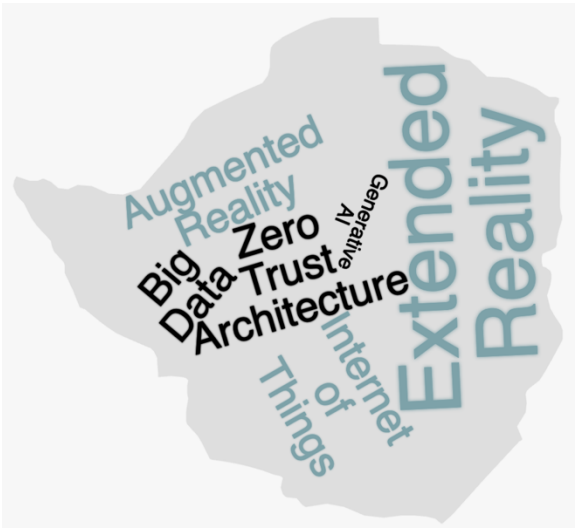


Figure 20 Emerging Technologies

As this is the first iteration of technology architecture work then the emerging technologies assessment work is skipped. The first iteration is to establish a steady baseline for technology architecture. This artefact should be filled (based on work done by stakeholders) during the second iteration of technology architecture development.

Table 21 Example Matrix of Monitored Emerging Technologies

Emerging Technology	Date of Assessment	Key benefits	Key threats	Position: Accept, Monitor or Ignore
Example: Generative AI	01.2025	Example: AI (as chat-bot) can automize processing of typical end-user questions.	Expects good and large amount of training data. Expects the solution owner	Monitor

Emerging Technology	Date of Assessment	Key benefits	Key threats	Position: Accept, Monitor or Ignore
			to understand the technology – skill limitation.	

4 Technology Architecture Building Blocks

As a result of the Technology Architecture work the identified building block – in Technology Architecture these are also called technology services. An illustrative overview of technology building blocks and their dependencies is provided in Figure 21.

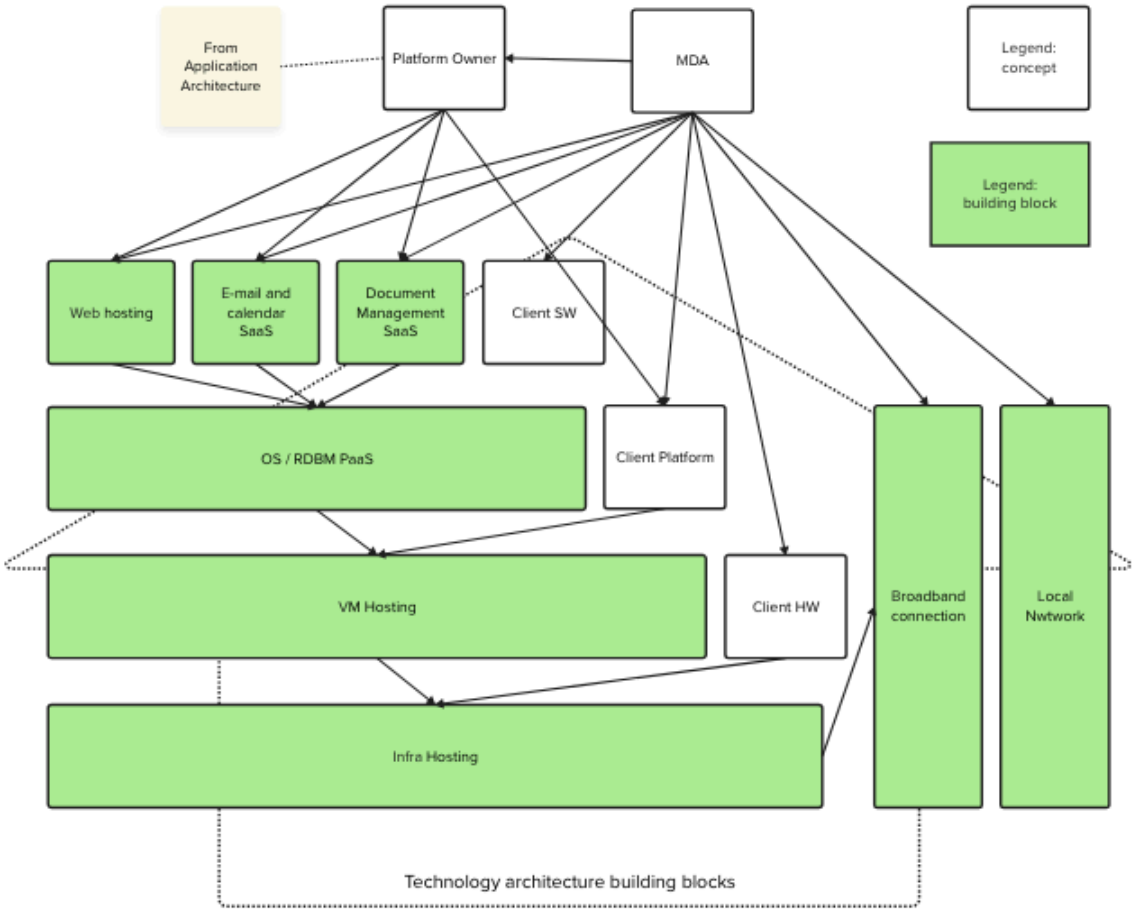


Figure 21 Technology architecture building blocks

While the building blocks of technology services in Zimbabwe seem to exist already, and there is no specific reason to create new technology services – there is still a significant need to revise and improve current services. For all existing technology services, the following problems must be resolved:

- The service owner (entity and department taking full responsibility for the service setup and operations) must audit its service and regular maintenance needs – this will be an input to make a budget request and or find alternative financing opportunities (for example, client fees). As a result, the technology services must be provided at a level that is financially and by human capacity

sustainable – a roadmap of activities for each service to capacitate and ensure stable operation must be composed.

- Establish platform SLA and commit – once the capability of the service is understood a realistic SLA must be declared and monitored. Taking a commitment to SLA usually means covering business losses for clients when SLA is not met... that would be the most effective approach to getting the necessary commitment but for understandable reasons, easier mechanisms might be deployed. The SLA of a service requires regular review and reassessment – is the service what the client needs, is the service what the service provider can provide, is the service what the service provider can commit?
- Client engagement – the service owner must establish client communication channels and practices to gather input on the satisfaction with the service and a way to help clients benefit more from the platform. Relevant metrics must be put in place for each service to measure how long clients wait to receive requested services, and how well the service fulfils its SLA.
- Currently, unreasonably high levels of custom-made solutions are used in the technology stack. It would be reasonable to minimize the usage of custom-made solutions for very standard and common requirements.

4.1 Building Block: Infrastructure Hosting

Service owner: NDC.

Service description: provide the secure room with power and network connection and cooling.

Considerations:

- The Service can be provided on several tiers depending on availability, recoverability and security – this would allow the service provider to ensure better cost efficiency.
- Define a cooperation model, relevant contracts and management mode to combine resources from the Ministry of Higher Education as part of the pool provided as infrastructure hosting to the clients.

4.2 Building Block: Virtual Machine Hosting

Service owner: NDC

Service description: provide virtual machines to clients from NDC infrastructure.

Considerations:

- Service can be provided on several layers depending on availability, recoverability and security.
- The service should be used also for other (higher level) technology services.

4.3 Building Block: OS / RDBMS PaaS

Service owner: NDC

Service description: Provide virtual machines for clients with a managed environment.

Considerations:

- Solutions that are provided using the PaaS model must be regularly monitored to provide those platforms that are required by clients.
- The PaaS model should be considered and used when the model is expected to provide an effect in terms of finances (benefit on patch license cost) or skills and capacity (the competencies and skills needed to platform are harder to find by MDAs).

4.4 Building Block: Web hosting

Service owner: GISP

Service description: government website hosting where MDAs can create web content, but the maintenance is handled by the service provider.

Considerations:

- The service should be built on top of Building Block: OS / RDBMS PaaS, Building Block: Virtual Machine Hosting or Building Block: Infrastructure Hosting.
- The solution currently used as a baseline should be reassessed to find best-fitting solution to be used for the web hosting service. The assessment should be done regularly in a couple of years intervals – if a better matching solution is found, the service should be migrated to avoid legacy problem creation.
- Training and support for MDAs must be coupled with the service to ensure smooth onboarding and high customer satisfaction.

4.5 Building Block: E-mail and Calendar SaaS

Service owner: GISP

Service description: hosted e-mail, calendar and other collaboration tools for MDAs and staff to use.

Considerations:

- Identify and select the best available collaboration toolset to be used for the whole of government.

- As the main tools for clerks, the availability of the service must match client expectations, and this is the responsibility of the service owner. Allowing (or making users through provision of inadequate service) user to rely on third-party services (Google, Yahoo, Hotmail etc.) is a security concern and should not be accepted.

4.6 Building Block: Document Management SaaS

Service owner: GISP

Service description: document and information management for SaaS.

Considerations:

- Find and possibly provide two solutions to be hosted and provided to avoid vendor lock-in and potential legacy issues.
- Establish a support mechanism to assist.

4.7 Building Block: Broadband Connection

Service owner: GISP

Service description: broadband connectivity for MDAs.

Considerations:

- Have the service owner define the front end for the customers.
- Cooperate with GISP and NDC for better content of service.
- Reasonable to cooperate with the private sector to be able to meet customer requirements.
- While reasonable security should be implemented the focus of security measures should be put on MDA information systems and platforms defined in application architecture.

5 Organisational View

The domain of technology in the context of ZWoGA requires better organisational arrangements. The most critical requirement is to establish a domain owner who would be responsible for general infrastructure and baseline technology challenges. The role will be responsible for:

- Government networking policies and services.
- Infrastructure requirements at NDC.
- Long-term planning of networking and infrastructure services and ensuring that the development of the domain supports digital transformation at MDAs.

The role would also become responsible for the Technology Architecture layer and its implementation not just considering strictly public sector resources but making sure that developments in the private sector are also aligning with ZWoGA's vision.

The second critical point is assigning a clear role and responsibility for networking services in the public sector. GISP must make clear its running costs and investment needs and with the Technology Architecture domain owner the resources must be found to enable service operation according to its client's needs.

6 Dependencies

The Technology Architecture domain is a baseline domain that is a physical enabler for all other ZWoGA domains. However, this increases its importance and it must also be understood that this domain should not be driving the digital transformation but rather support all MDAs in their digital transformation with sufficient and good services.

The following key relationships between other architecture domains are foreseen:

- Integrated Public Service Architecture
    - Service design methodologies must consider available services from technology architecture to design services that can be implemented.
    - The IPS architecture must be seen as the main domain defining requirements and expectations for Technology Architecture.
    - Using the emerging technologies (Artefact: Emerging Technologies Matrix) the Technology Architecture domain can assist IPS architecture in finding use cases for emerging technologies that are about to be adopted.
- Application Architecture
    - Application and Technology Architecture from ZWoGA's perspective must be seen and domains supplementing each other's services for MDAs to be able to focus on their changes.
    - Platform owners from application architecture must be able to provide further input to Technology Architecture about the future requirements imposed on infrastructure and networking.
    - Using the emerging technologies (Artefact: Emerging Technologies Matrix) the Technology Architecture domain can support application architecture to establish new platforms that allow the uptake of emerging technologies for a wider set of MDAs.
- Data Architecture
    - Technology Architecture can be seen as one of the key entry points for collecting the systems and services owned and used by MDAs.
    - When designing meta-data collecting methods and solutions in Data Architecture, the Technology Architecture domains must be seen as critical stakeholders for the information-gathering process.
- Security Architecture
    - The methodology of security appointed in Security Architecture must be followed also by all services in technology architecture.
    - The networking services must cooperate with the Security Architecture – supervision and monitoring-related building blocks must have good alignment with networking services to be able to deliver their value to the ecosystem.

- Governance architecture
    - Technology Architecture must surrender to the general management structure of the ZWoGA.

Delivering a seamless Government experience

D4-5 Data Architecture

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Acronyms

Acronym	Full text
ABB	Architecture Building Blocks
G2B	Government to Business
IPS	Integrated Public Service
IS	Information System
MDA	Ministries, Departments and Agencies
OPC	Office of the President and Cabinet
ToT	Training of Trainers
ZWoGA	Zimbabwean Whole of Government Architecture

1 Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the " An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for Enterprise Architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to Enterprise Architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

Data architecture **defines what kind of data is needed and collected** to support the implementation of ZWoGA. It offers information necessary for service design and redesign, management decisions and risk management. Data Architecture refers to the structured information listed in different catalogues like public service catalogues, and catalogues of Government institutions.

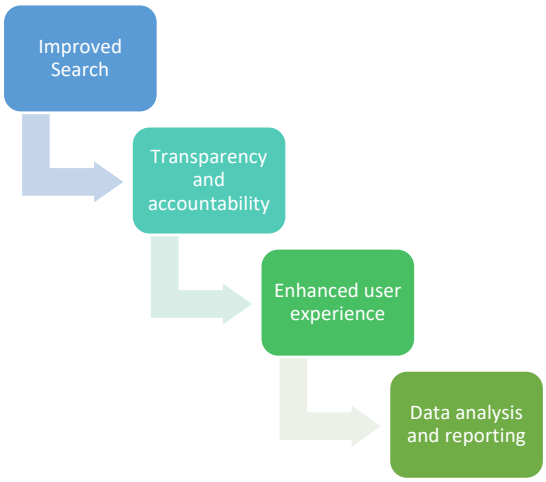


Figure 22 Benefits of Data Architecture

This creates transparency in the public sector and standardization **enables better integration, interoperability, and alignment of services** with overarching government goals and strategies, ultimately enhancing efficiency, transparency, and effectiveness in service delivery. The benefits of the agreed Data Architecture are the following:

- A well-defined structure allows for efficient searching based on various criteria.
- Clear and detailed information fosters public trust in government services.

- Users can easily find the information they need, leading to a more positive experience.
- Standardized metadata eases data gathering and reporting on service usage.

Data Architecture is tightly linked to other architecture domains, providing necessary information for designing Integrated Public Services (IPSs), application architecture, and technology architecture.

The current document describes the Data Architecture domain, building blocks, organisational view, and dependencies with other ZWoGA domains. Implementation of the described principles, building blocks and enablers will help Ministries and other Government institutions provide better services.

The current document is addressed to heads of IT departments, service owners, data owners, business analysts, technical architects, and everyone else involved in designing and implementing public services:

1. Public Sector Reforms and Performance Management Department.
2. Public officials engaged in the projects of designing and developing digital public services at both executive and administrative levels (e.g., services, G2B services).
3. Public officials engaged in the projects of digitalizing data and developing data exchange services at both executive and administrative levels.
4. Public officials overseeing change management and capacity building.
5. The Ministry of ICT, Postal and Courier Services.

This document describes the Data Architecture as a core source of information and meta-data for other architecture domains to support the implementation of ZWoGA, the document includes the architecture domain (Chapter 2), building blocks (Chapter 4), organisational view (Chapter 5), and dependencies (Chapter 6).

2 Data Architecture Domain

The Data Architecture domain is a foundational part of the ZWoGA, holding an overview of different meta-data catalogues and answering questions about whom, how and what matters to contact.

Well-designed meta-data catalogues and management systems support architecture implementation and governance as one domain, ensuring a high-quality WoGA.

Meta-data practices found by the MDAs are:

1. **COMPATIBLE:** metadata must be as open, interoperable, scannable, machine-actionable, and human-readable as possible. There should be no privacy or confidentiality factors in meta-data.
2. **COMPLETE:** metadata must be as complete and comprehensive as possible. As much as needed, as little as possible - stands as a good practical guideline in this perspective.
3. **CREDIBLE:** metadata must be of clear provenance, trustworthy, accurate and timely.

CURATED: metadata must be kept over time. Administrative processes, service provision, data management and decision-making must be transparent and MDA staff members are the main users.

Data architecture artefacts are:

1. Catalogue(s) of meta-data (see Chapter 44).
2. Process of meta-data collection (see Chapter 5).
3. List of quality constraints (see Chapter 3).
4. Motivation of stakeholders (see Chapter 5).

3 Artefact: Quality Constraints

Metadata quality constraints are:

1. Missing or incomplete metadata.
2. Inconsistent or conflicting metadata.
3. Outdated or inaccurate metadata.
4. Non-standard meta-data.
5. Poorly defined metadata.

These constraints can lead to problems in finding and interpreting data, cause confusion, lead to wrong or misleading data analysis and decisions, and reduce the interoperability and usability of data.

Improving the quality of metadata involves the following strategic measures:

Table 22 Strategic measures for improving metadata quality.

Quality constraint	Improvement measures
Missing or incomplete metadata	Establish mandatory fields for all metadata records to ensure these fields are populated before records can be considered complete. Implement automated validation checks to find missing metadata fields and flag incomplete entries for correction. Develop guidelines for metadata entry to ensure all necessary information is consistently captured. Conduct regular audits of metadata to find and address gaps in completeness.
Inconsistent or conflicting metadata	Define and enforce standards for metadata, including naming conventions, formats, and controlled vocabularies. Use automated tools to perform consistency checks across metadata entries. Flag and resolve conflicts. Provide training to staff on metadata standards and best practices to reduce inconsistencies.
Outdated or inaccurate metadata	Schedule regular updates to review and refresh metadata entries to ensure accuracy and relevancy over time. Use automated alerts to notify data stewards when metadata needs updating.

Quality constraint	Improvement measures
	Regularly verify metadata against authoritative sources to ensure accuracy.
Non-Standard metadata	Use compliance tools to check metadata entries against established standards. Provide guidelines and templates to standardize metadata entry across the organization. Conduct interoperability testing to ensure that metadata conforms to standards and can be effectively used across different systems.
Poorly defined metadata	Develop clear definitions and documentation for all metadata fields. Engage with stakeholders to ensure that metadata definitions meet their needs and are clearly understood. Regularly review metadata definitions and incorporate feedback to refine and improve clarity.

4 Building Blocks

Data Architecture holds a list of catalogues relevant to other architecture domains:

1. Organisations (MDAs)
2. Public Services
3. Information Systems

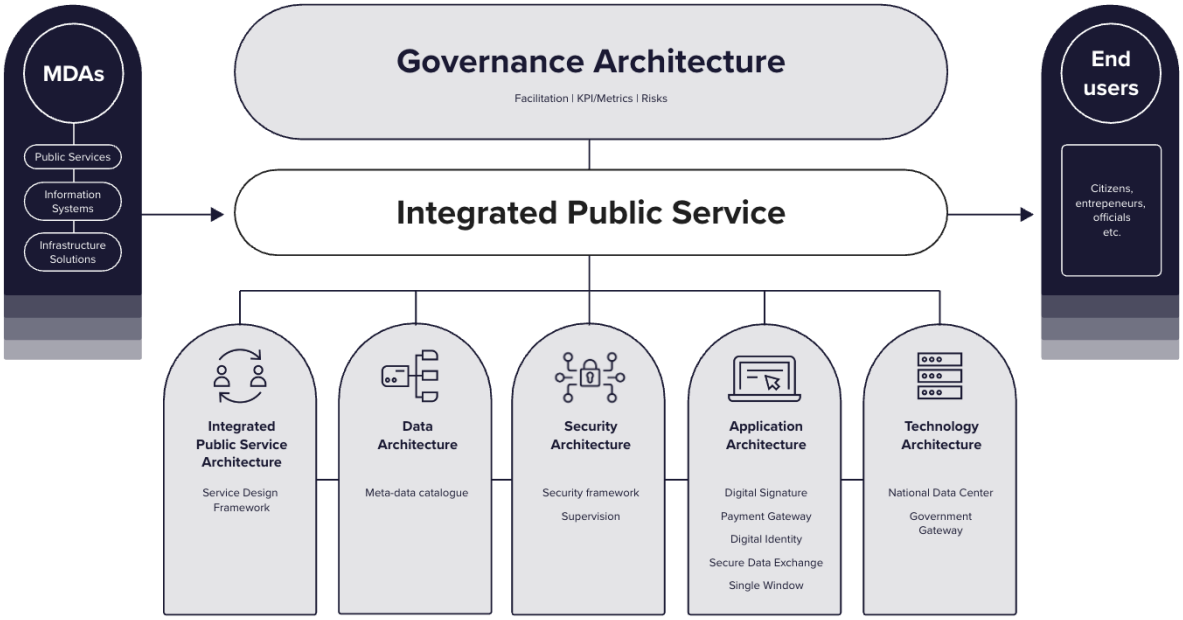


Figure 23 Zimbabwean Whole of the Government Architecture

4.1 Catalogue of Organisations

The purpose of the catalogue of organisations is to capture a definitive listing of all participants that interact, including users and owners of IT systems (applications), data and services.

The catalogue of organisations includes the following data:

Table 23 Content of the catalogue of organisations.

Meta-data field	**Description**	**Use-case / Purpose**
General data	General information about organization	
Name	Full official name of organization	For all users/ Allows to find about who the data is about

Meta-data field	Description	Use-case / Purpose
Acronym or short name	Short name or code of organization	For all users
Registration Number	Official identifier of organization given by government	For all users/ Allows to find about who the data is about
URL	Link to the organization's official website	For all users / Allows to get more information about the subject
Description	Description of organization and its key functions	For all users / Allows to get more information about subject's goal and functions
Type	Legal statute of the organisation and its type (e.g., Central Government; State Institution, Public Body, Local Government, Local Government Body, Private Body, NGO, Other).	Governance - distinguish what legislation and governance mechanisms apply to the institution. MDAs - finds the mode of cooperation
Contact Persons	General information about the contact person in organization considering meta-data about the organisation and its assets.	
Name	Name of contact persons	For MDAs / Allows to contact in case of more questions
E-mail	Official e-mail of contact person	For MDAs / Allows to contact in case of more questions
Phone/WhatsApp	Official phone of contact person	For MDAs / Allows to contact in case of more questions

4.2 Catalogue of Public Services

The purpose of the public services catalogue is to provide information about services provided by each MDA. The catalogue of public services includes the following data:

Table 24 Content of the catalogue of public services.

Meta-data field	**Description**	**Use-case / Purpose**
General data	General information about service	
Name	Name of service	For all users/ Allows to find the service
Identifier	Short name or code of service	For all users/ Allows to find the service
Description	Service description	For all users/ Allows to understand the purpose of the service
Channels	Service delivery channels (e.g. On-site, post, phone hotline, e-mail, website)	For all users/ Gives information about service provision channels
Personal Data	Attribute showing whether service includes personal data and/or sensitive data	For all users /Refers to if personal data is processed or not
Service URL	Link to the website if available	For all users/ Allows to get more information about the service or to start using the service
Service Level Agreements		
Service Availability and uptime	Description of service working hours	For all users/ Provides information about working hours for both digital and non- digital services.
Contact Persons		
Name	Name of contact persons	For MDAs/ Allows to contact in case of more questions
E-mail	Official e-mail of contact person	For MDAs/ Allows to contact in case of more questions

Meta-data field	Description	Use-case / Purpose
Phone	Official phone of contact person	For MDAs/ Allows to contact in case of more questions

4.3 Catalogue of Information Systems

The purpose of the Information Systems (IS) catalogue is to provide information about applications and datasets collected and stored in them. Catalogue of information systems includes the following data:

Table 25 Content of the catalogue of information systems.

Meta-data field	Description	Use-case / Purpose
General	General information about service	
Description	Description of IS.	For all users/ Describes the main aim of the IS
Name	Name of information system	For all users / Allows to find the IS
Identifier	Short name or code of information system	For all users / Allows to find the IS
Related Institution		
Name	Name of the institution managing the IS	For all users / Allows to find organisation responsible for managing IS
Link/URL	URL or internal catalogue link to the related solution	For all users / Allows to get more information of the organisation managing IS
Contact Persons	Person responsible for the information system.	
Name	Name of contact persons	For MDAs / Allows to contact in case of more questions
E-mail	Official e-mail of contact person	For MDAs / Allows to contact in case of more questions

Meta-data field	Description	Use-case / Purpose
Phone	Official phone of contact person	For MDAs / Allows to contact in case of more questions

5 Organisational View

The data architecture owner is, and its implementation is coordinated by the E-Government Technology Unit under OPC. Significant cooperation is expected between OPC and POTRAZ for meta-data collection and systemization as the needs are quite well aligned.

Capacity-building activities for MDAs to adopt and implement data architecture are done in cooperation with the Public Service Commission (e.g., development of online courses).

5.1 Meta-data Collecting Process

While the e-Government Technology Unit handles coordinating the meta-data collection process, including creating and managing solution(s) for meta-data catalogues, MDAs stay responsible for the quality of meta-data since they are entering respective information into the catalogues. Each MDA must make sure that meta-data about their information systems, services and other information entered in the catalogue(s) is up to date.

Stakeholders can be motivated using the following approach:

1. Service and data digitalisation activities for MDAs are supported and funded by the government only if the meta-data is up-to-date and reflects the actual situation.
2. MDAs can refer to existing catalogues in case information is needed by others and avoid continuing explanations about what kind of services they are offering and what data they are collecting.

The meta-data collection process is continuous and includes the following steps: '

1. The first input of meta-data: this is the first submission of data by the MDAs after the catalogue is created. The E-Government Technology Unit will set a due date and check that meta-data is entered properly and prompt.
2. Updating meta-data: since data about services, organisations and information systems may change during the time, MDAs are bound to update respective information. The E-Government Technology Unit will also introduce a process to coordinate regular reviews and supervision of meta-data catalogues.

5.2 Meta-data Quality Management

MDAs must ensure meta-data quality by following the following steps:

1. Assessing and measuring the completeness, accuracy, consistency, timeliness, and compliance of meta-data.

2. Improving meta-data quality by correcting, removing, or enhancing the meta-data that is missing, inconsistent, outdated, or inaccurate.

The e-Government Technology Unit under OPC will support MDAs during the meta-data collection, data digitalization, design, and development of integrated public services by creating related methodologies, making available necessary tools, and creating a learning environment together with a knowledge base.

Implementation support by the unit means:

1. Improving the cataloguing solution to enhance the quality of meta-data at entry.
2. Conducting different capacity-building programs.
3. Conducting ToT programs for MDAs where digitalisation is stronger.

MDAs are expected to:

1. Adjust their internal work processes in such a way that implementation of ZWoGA is supported.
2. Assign specific people responsible for managing meta-data and keeping it up to date.
3. Allocate sufficient funds needed for data architecture development, data governance and data management.
4. Support and take part in capacity-building programs.
5. Participate in different working groups, sharing knowledge (both success stories and failures), and giving feedback on the architecture implementation.

6 Dependencies

All domains and components of the ZWoGA are linked and developed to support the whole digital government ecosystem (see Figure 23).

Additionally, building blocks of different domains and enablers (foundational projects) are tightly linked to data architecture, as described below:

i) IPS architecture:
   (1) Designing IPS relies heavily on what is available from other MDAs - information about what data is being processed by other entities is needed when designing or redesigning public services.
   (2) Data can be used or reused if it is in digital format. Data architecture sets up principles for how digital data should be stored, described, and shared.

ii) Application Architecture:
   (1) Data exchange requires information about organisations and their information systems - the discoverability property of data, services, systems, and organisations is generic for different applications at the whole government level and therefore discovery mechanism should not be part of data exchange, but rather generic functionality provided from data architecture.
   (2) Identity (digital and not digital) of persons and how data in MDAs is linked to persons is critical knowledge when designing digital public services - where and what data is linkable to persons.
   (3) Data Architecture provides a means for finding what systems process and keep personal data. (Digital) identity from application architecture ensures that persons and their data are linkable.
   (4) When providing services, it is important to know who is behind the screen or who is using the mobile phone to apply. Application architecture creates rules and requirements for secure authentication (digital identity) and digital signing so these components can be integrated into digital services.

iii) Security Architecture:
   (1) When digitalising and sharing data, cross-functional requirements need to be considered. The role of data architecture is to provide an up-to-date overview of MDAs and their systems for security architecture to build an understanding of what and where essential information and ICT assets are- discoverability.

iv) Technology Architecture:
   (1) When digitalising data, requirements for the technology and an agreed approach to a technical solution must be considered.
   (2) Technology Architecture, on the other hand, must consider the needs and expectations of service design and data sharing to provide the best services to end users.

v) Joint components of each domain:

(1) **Legal framework** - the legal framework will provide a clear understanding of how to find the authentic and sole controller of data, as having multiple controllers for the same dataset is a factor slowing down digitalization and interoperability efforts.
(2) **Financing** - a clear agreement on how the development and management of public services together with data digitalisation are financed is part of the ZWoGA.
(3) **Discoverability** - the data architecture is expected to provide discoverability of stakeholders, systems and services for all other functionalities that are needed by other architecture domains.

Learning Programme for Sample Learning Programme for Data-Driven Decision-Making for Mid-Level Management is described in chapter 9.11 of the Change Management Strategy.

Delivering a seamless Government experience

D4-6 Security Architecture

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Content

Index of Tables

Definitions

Term	Definition
Confidentiality	Unavailability or non-disclosure of information to unauthorized persons, entities or processes. One of the three main components of information security, denoted by the letter C in the abbreviation C-I-A.
Integrity	The correctness and completeness of the information, the absence of unauthorized changes, also includes authenticity and non-repudiation. One of the three main components of information security, denoted by the letter I in the abbreviation C-I-A.
Availability	The property of information to be available and usable at the request of an authorized entity in a timely manner. One of the three main components of information security, denoted by the letter A in the abbreviation C-I-A.
Data at rest	Data at rest is data that has reached a destination and is not being accessed or used. It typically refers to stored data and excludes data that is moving across a network.
Data in transit	Data in transit is data that is being transferred between locations over a private network or the Internet. As example, an email sent / received from one user / server to another is data in transit.
Loss	Measure of unwanted change, basic component of risk analysis, primary factor determining the need for information security.
Data loss	It where data is destroyed, deleted, corrupted, or made unreadable by users and software applications.
Threat	Potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.
Risk	The threat's ability to cause loss / harm to the organization. The current or prospective risk of losses due to the inappropriateness or failure of the hardware and software of technical infrastructures, which can compromise the availability (accessibility), integrity, and security of such infrastructures and of data.

Term	Definition
Information Security Management System	Set of policies, procedures, guidelines, and related resources and activities that an organization collectively manages to protect its information assets. It is based on the consideration of risk and its acceptance to levels that ensure effective handling and management of risks.
Information Security Policy	The organization's central information security document, which stipulates development directions and desired goals, determines what is allowed and what is not allowed.

Acronyms

Acronym	Long text
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incidence Response Team
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer.
GCISO	Government Chief Information Security Officer.
ICT	Information and Communications Technology.
IPS	Integrated Public Service.
IS	Information System.
ISACA	Information Systems Audit and Control Association.
ISMS	Information Security Management System.
SABSA	Sherwood Applied Business Security Architecture.
SOC	Security Operation Centre.

Acronym	Long text
WoG	Whole of Government.
WoGA	Whole of Government Architecture.
ZWoGA	Zimbabwean Whole of Government Architecture.

• Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the "An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for Enterprise Architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to Enterprise Architecture development within the Government of Zimbabwe. It aims to contribute to a successful realization of the country's digital transformation goals by providing a comprehensive framework and guiding principles.

Cybersecurity is a growing and widely diffused complex threat to Zimbabwe in many ways. The severity of security demands brings into question Zimbabwe's approach in this fifth 'domain' of warfare.

Zimbabwe's precarious state in the cyber domain is seen by its ranking of 119 out of 160 countries in terms of the National Cyber-Security Index (NCSI), a measure of how countries are prepared to prevent cyber threats and manage cyber incidents (NCSI, 2021). The country is deficient in aspects of detecting, identifying, deterring, and protecting against threats emanating from the cyber domain[3]. Please see the Legal Review for more detail on the legal aspects of the issues dealt with in this report.

The crafting of the Cybersecurity Policy must be inclusive, involving traditional Security Architecture and other nontraditional players such as OPC, MICTPCS, MHTESTD, civil society, and the private sector.

The Security Architecture, one of the selected areas of the ZWoGA is oriented toward the team responsible for preparing and running the security architecture development.

It is expected to be relatively a small team (architects of MDAs, members of the Cybersecurity Committee) that runs the architecture work preparation led by an experienced Government Chief Security Officer (GCISO), who needs to prepare and run the security architecture work. Such a team might be informal in the beginning, following the clarification of roles and mandated organizational structure.

[1] https://silveirahouse.org.zw/wp-content/uploads/2022/10/Cyber-Policy-Brief-Proof_2.pdf

Methodology, supervision - the document should be used as a baseline to guide the team in preparing and steering the security architecture process. The team should revise the **methodology** and adjust it according to the specific needs of the expected architecture iteration.

It is essential to monitor and **supervise**, that the approach handled by this methodology should cover the whole of the government, and to ensure that all stakeholder's interests are covered, and the development of security architecture is balanced.

ZWoGA Security Architecture suggests a standardized approach for implementing security measures and emergency response capabilities to keep MDAs and their information systems security aware while digitalizing data, developing applications, and using technologies to create Integrated Public Services (IPS) between MDAs and citizens.

Chapters of this document are outlined as follows:

- **Chapter** Error! Reference source not found. Error! Reference source not found. – introduces Security Architecture scope, and stakeholders with attaching aspects resulting from the Architecture development workshop conducted in April 2024.
- **Chapter ☐ Inception** - as the starting position is modest for Security Architecture then some critical initial foundational aspects are brought out in a dedicated chapter. Aspects of Security Architecture that create the baseline for all future Security Architecture iterations.
- **Chapter 7 Security Architecture Building Blocks** – presents various Security Architecture building blocks.
- **Chapter 8 Security Architecture Artefacts** – presents various artefacts and explains the necessity for the ZWoGA. This chapter also outlines the agreed ZWoGA goal by MDAs and explains how the planned Security Architecture will achieve set objectives and address key concerns.
- **Chapter 9 Organisational view** – gives organizational view to implement and manage the Security Architecture in theory.
- **Chapter 10 Dependencies** – clarifies the dependencies between Security Architecture and other architectures within ZWoGA.

• Security Architecture Domain

Cybersecurity is a domain dealing with policies, tools, guidelines, methodologies, standards, etc. that can be used to protect the assets in the cyber environment. Such assets include connected personnel, infrastructure, applications, services, telecommunications systems, and most importantly information in digital form. The Cybersecurity domain addresses itself as a critical component for real-life safety. Cybersecurity strives to ensure the attainment and maintenance of digital solutions with the security properties built into the solutions.

The Security Architecture, as the conceptualizing and modelling paradigm, provides:

- Conduct risk and value-based assessments.
- Support solution creation and operation with security consideration built-in to the core solutions.
- Provide a reproducible unified security design for the whole of government.
- Identifying critical policies, rules, and regulations to enforce security concepts for stakeholders.

The following concerns related to security were exposed by stakeholders from workshops held in Zimbabwe in April 2024. The Security Architecture has been developed to address those concerns.

Table 26 List of Security-related Concerns

Concern
Job security
Security of the system
Cybersecurity (CIA) - concerns about identify theft and ransomware
Cybersecurity of information (e.g. disaster recovery)
Cybersecurity concerns: confidentiality, integrity, availability, data privacy
Privacy or security of taxpayer information
Data security and privacy

○ Baseline Concepts

As the key asset of Cybersecurity is information and its protection the following concepts are considered as agreed upon by the stakeholders as a set of baseline concepts.

▪ CIA Triad

The CIA Triad – **Confidentiality**, **Integrity**, and **Availability** – forms the backbone of Security Architecture, ensuring data protection and availability. In the context of building Integrated Public Services (IPS) with digital means, data protection plays a critical role.

Authentication verifies that the user attempting to access a system is who they claim to be. This may be accomplished through a combination of credential solutions. The strength of the credential system (usernames and passwords combined with One-Time Passwords, Tokens, Biometrics, Certificates, etc.) must be aligned with the resources that are being accessed. Preferring stronger authentication mechanisms as universal authentication methods (usable also for accessing resources that do not expect strong authentication) is the preferred approach.

Access Control and Authorization are to allow access to resources only to authorized individuals. The white-list approach (list of for whom access is granted) should be preferred although for certain use cases, the black-list approach (list of whom access is denied) can also be considered appropriate. It is critical that the entity controlling access to the resources in real life would also have the responsibility to control the access in the cyber environment.

Data Confidentiality is closely related to authorization - it refers to requirements and measures to maintain the privacy of information while in storage (data at rest) or is being transmitted (*data in transit*). While authorization mechanisms handle most cases of stored data the data in transit is slightly more complicated - this is usually accomplished by encryption, with suitable algorithms.

Data Integrity ensures that data at rest or in transit is not changed without permission and changes are discoverable.

Non-repudiation is critical for data in transit - on top of integrity protection and tamper-proofing the data non-repudiation means coupling integrity-protected data with its source using cryptographical mechanisms that would give data recipient insurance that the data provider cannot back up from shared data. This is in most cases handled with cryptography-based signature or seal mechanisms and allows the recipient of data to automate their processes as external information sources can be used as evidence if there are any disputes.

Availability is about making sure that data is available when needed.

▪ Zero Trust

The Zero-Trust Security Model[4], also known as Zero Trust Architecture (ZTA), Zero-Trust Network Access (ZTNA), and perimeter-less security describes an approach to the strategy, design, and implementation of IT systems. The main concept behind The Zero-Trust Security Model is "never trust, always verify", which means that users and devices should not be trusted by default, even if they are connected to a permitted network such as a corporate LAN and even if they were previously verified.

ZTA is implemented by establishing strong identity verification, validating device compliance before granting access, and ensuring least privilege access to only explicitly authorized resources. Most modern corporate networks consist of many interconnected zones, cloud services, and infrastructure, connections to remote and mobile environments, and connections to non-conventional IT, such as IoT devices.

The reasoning for zero trust is that the traditional approach – trusting users and devices within a notional "corporate perimeter", or users and devices connected via a VPN – is not sufficient in the complex environment of a corporate network. The zero-trust approach advocates mutual authentication, including checking the identity and integrity of users and devices without respect to location and providing access to applications and services based on the confidence of user and device identity and device health in combination with user authentication. The Zero-Trust Architecture has been proposed for use in specific areas such as supply chains.

The principles of zero trust can be applied to data access and the management of data. This brings about zero trust in data security where every request to access the data needs to be authenticated dynamically and ensure the least privileged access to resources. To determine if access can be granted, policies can be applied based on the attributes of the data, who the user is, and the type of environment using Attribute-Based Access Control (ABAC). This zero-trust data security approach can protect access to the data.

○ Security Architecture Vision

Successful Security Architecture implementation requires dealing with Cybersecurity from several aspects at the same time.

- Establishing a **clear and compelling Security Architecture vision** and strategy that aligns with the business goals, risks, and requirements (e.g., CIA triad, Zero Trust).
- Agree and **document the Security Architecture principles, standards**, patterns, models, guidelines, policies, procedures, and controls.

[2] https://en.wikipedia.org/wiki/Zero_trust_security_model

- Establish a **Security Architecture team** empowered with the skills, knowledge, and authority to develop, review, approve, implement, maintain, and change the Security Architecture. This can be a virtual team built by information security officers (CISO) from several MDAs.
- Implementing and **monitoring a Security Architecture governance process** that follows a consistent approach to Security Architecture development is necessary.
- **Measuring and reporting on the Security Architecture governance metrics** can assess the performance and outcomes of the Security Architecture governance.
- Encouraging the **adoption of best practices, legal requirements** to use such practices can be made in different legislation, as discussed in the Legal Review.
- **Awareness building** for a wider set of stakeholders as the in-experienced users are those who are targeted the most with attacks.

○ Stakeholders

The following stakeholders are critical for establishing a sustainable and resilient Cybersecurity approach:

- **Government Chief Information Security Officer (GCISO) -** owner of the Security Architecture domain. Responsible for the strategic direction and prioritization of the GoZ's approach to Cybersecurity. The GCISO draws on the technical expertise, relationships, and unique insights from other Cybersecurity-related domains to uplift information security practice across the government. Fulfilment of the role of GCISO might be informal.
- **CISOs or Security Architects from MDAs** - role in MDAs having an overview of security adoption and processes in an MDA.
- Representatives of NCIRT.
- **Data Protection Officer of MDA** - ensure that MDA processes the personal data of its staff, customers, providers, or any other individuals/citizens (also referred to as data subjects) in compliance with the applicable data protection rules.
- **Supervising authority** - separate entity or unit, where independence from CISOs and Security architects is ensured.
- The Cybercrime Unit within the Commercial Crimes Division (CCD) of the Zimbabwe Republic Police.

• Inception

The Cyber and Data Protection Act of 2021[5] (Preliminary Act) was supposed to create two new entities: (1) the Data Protection Authority (DPA) as a unit within the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) and (2) Cybersecurity and Monitoring of Interception of Communications Centre as a unit within the Office of the President and Cabinet (OPC).

They were planned to oversee advising the MICTPCS on matters relating to the right to privacy, access to information, and Cybersecurity, conducting research on policy and legal matters as well as facilitating cross-border cooperation relating to data protection and Cybersecurity.

However, the component of Cybersecurity was dropped during a debate in parliament, therefore the preliminary act cannot be referred to as a law on Cybersecurity.

Data Protection Act [Chapter 11:12] No. 5/2021[6] was introduced. Designation of the Postal and Telecommunications Regulatory Authority (POTRAZ) as the Data Protection Authority cooperates with the Consumer Protection Commission as well as the Competition and Tariffs Commission.

In other words, Zimbabwe does not have a Cybersecurity law. The Zimbabwe Republic Police does not have a specified department or unit dedicated to cybercrime yet. No National Computer Incident Response Teams (CIRT) in Zimbabwe has been created yet.

Therefore, the initial work for establishing necessary security-related entities and agreements requires also the Security Architecture to define different approaches for the initial Security Architecture building. The elements - core building blocks for Security Architecture - described below will provide a baseline also for future Security Architecture iterations.

○ Cybersecurity Leadership

For Zimbabwe, to benefit from the social and economic promise of digitalisation, it must manage the accompanying risks and threats strategically at the highest level. A solid Cybersecurity governance framework at the national level, with a clear allocation of roles and responsibilities, and coordination mechanisms, raises preparedness and resilience across all sectors and levels of society. A national Cybersecurity strategy establishes the

---

[3] https://www.ictministry.gov.zw/wp-content/uploads/2024/01/Cyber-and-Data-Protection-Act-Chapter-1207.pdf

4 https://www.potraz.gov.zw/wp-content/uploads/2022/02/Data-Protection-Act-5-of-2021.pdf

key national objectives and priorities and drives systematic planning and accountability by laying down the implementation modalities in an action plan.

Without clearly identified political leadership at the highest level, Cybersecurity does not get represented in political decision-making. A lack of representation in turn leads to a lack of Government ownership, accountability, and appropriate resources.

The organisation and Cybersecurity leadership responsibility for Cybersecurity must be formally assigned at the highest governmental or political level. Ideally, this should be assigned permanently through legislation or national strategy to a position or institution exercising the country's executive power with a governmental mandate, such as the cabinet, a government minister, or a ministry.

GCISO requires a body composed of key stakeholders. Such a body should include stakeholders from the public and private sectors and selected representatives from civil society organisations. Implementing Security Architecture requires the existence of an officially recognized mechanism - a permanent committee, council, working group, etc. - that regularly revises the progress of Security Architecture implementation and resolves challenges encountered on this path.

The members of such a body could include the representatives from following entities:

- Ministry of ICT, Postal and Courier Services (MICTPCS).
- Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ).
- Ministry of Higher and Tertiary Education, Innovation, Science and Technology Development (MHTESTD).
- Ministry of Justice, Legal and Parliamentary Affairs (MJLPA).
- National Computer Incident Response Team (NCIRT).
- Zimbabwe Republic Police (ZRP).
- National Prosecuting Authority (NPA) / Zimbabwe Anti-Corruption Commission (ZACC).
- Ministry of Defence (MOD).
- Central Intelligence Organization (CIO) of Zimbabwe.
- Any representative from any sector of the economy or any other person who may be necessary to the deliberations in respect of a particular warrant.

Security Framework

Building on the existing experience it is reasonable to identify and select an internationally well-established framework or methodology as the baseline that will be adopted in Zimbabwe by all MDAs as the Zimbabwean Security Framework.

While the list below does not present a complete list of all potential security frameworks it is most effective to use some international standard or framework as this would allow benefiting from the ecosystem of experts related to specific frameworks and save time as customizing a framework is more efficient than establishing one from scratch.

- **ISO/IEC 27000 family** - The ISO/IEC 27000-series, also known as the "ISMS Family of Standards" or "ISO27K" for short, comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
  The series provides best practice recommendations on information security management – the management of information risks through information security controls –within the context of an overall Information Security Management System (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series), environmental protection (the ISO 14000 series) and other management systems.
  From the long list from the series, the two related to ICT must be emphasized: ISO/IEC 27001:2022: Information Security Management and ISO/IEC 27557:2022 – application of ISO 31000:2018 for organizational privacy risk management.
- **SABSA** - the Sherwood Applied Business Security Architecture, is a policy-driven framework. It helps define the critical questions that Security Architecture can only answer: what, why, when, and who. The goal of SABSA is to ensure that after the design of security services, they are then delivered and supported as an integral part of the enterprise's IT management. One downside, however, is that SABSA doesn't get into specifics regarding technical implementation.
- **NIST** - The NIST Cybersecurity Framework is designed for individual businesses and other organizations to assess the risks they face. It is set forth by the National Institute of Standards and Technology (NIST) under the United States Commerce Department. The framework helps organizations implement processes for identifying and mitigating risks and detecting, responding to and recovering from cyberattacks. It is recommended for any organization that wants to enhance its Cybersecurity risk management practices.
- **OSA** - Open Security Architecture (OSA) is a framework related to technical and functional security controls. OSA offers a comprehensive overview of crucial security components, principles, issues, and concepts that underlie architectural decisions involved in designing effective Security Architectures. However, OSA can only be used if the Security Architecture has already been designed.
- **COBIT** - the Control Objectives for Information and Related Technologies, is a framework created by ISACA for Information Technology (IT) management and IT governance. The framework is business-focused and defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process activities, process objectives, performance measures, and an elementary maturity model.

The security framework must be complemented with a supervision function - an entity or unit that supports MDAs in adopting the Security Framework and can carry out audits on the implementation.

○ Information Security Management System

An Information Security Management System (ISMS) is an overview of practices and procedures for systematically managing an organization's sensitive data. An ISMS must be established by each MDA following the general instructions from the Security Framework.

In ISMS an organisation describes relevant people/roles, information assets the procedures to be followed to ensure the safety of high-value information assets (including data) within the organization for normal operation. The ISMS must refer to the incident response plan as this is a specific instrument for handling an incident.

The main targets for the ISMS are:

- Implementors: Information Security Managers, Business Process Managers, Unit Managers, IT Employees,
- Auditors, and
- Consultants.

Parts of the ISMS can be used as a manual in the development, administration or learning processes of IT systems

7 Security Architecture Building Blocks

7.1 Monitoring and Incident Response

The IETF RFC 2350[7] specifies what is expected of a National Computer Incident Response Team (NCIRT). The basic tasks of an NCIRT include monitoring cyber incidents at the national level, providing early warnings, alerts, announcements and information to relevant stakeholders about risks and incidents, responding to incidents, and participating in the CSIRT networks. To further strengthen the monitoring capability dedicated teams or units (Security Operation Centres or SOCs) can be formalized within or nearby NCIRT.

An NCIRT should clearly define its constituency and publish information about its services and communication channels. Services provided by an NCIRT can be divided into two broad categories:

- real-time activities directly related to their main task of incident response and
- proactive activities in support of the incident response task.

Appropriate national incident response capabilities are a central constituent of national cyber resilience. A dedicated, adequately resourced national CSIRT can significantly lower cyber risks to a country's economy and society by providing proactive and preventive services. In the event of a cyber incident, national CSIRTs coordinate incident response at the national and international levels, thereby helping to minimise damage and recover quickly from the incident.

Cooperation with the Zimbabwe Republic Police is critical for the monitoring and incident response provider.

For additional information, the ENISA publication "How to set up CSIRT and SOC"[8] provides good clarification.

7.2 Critical Information Infrastructure Protection

Information systems and digital services are an inseparable part of Zimbabwe's infrastructure that allows societies to function. Some of these infrastructure elements are considered critical: their disruption or destruction could have a serious impact on the normal day-to-day life of the society - banks, hospitals, electricity, clean water, etc. Many such systems are dependent on ICT – Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) applications, or other digital solutions, services or processes – some of which are critical to the operation and

[5] https://datatracker.ietf.org/doc/html/rfc2350
[6] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

continuity of the Critical Information Infrastructure (CII) or Critical Infrastructure (CI) itself. It is a matter of public safety and national security to have established mechanisms to manage such risks and prevent them from materializing.

For CII protection a continuous methodology for identifying operators of CII and vital service providers is needed. The CII operators must fall in the category where Cybersecurity-related requirements are made mandatory (even if those are private sector entities) and competent supervisory authority established.

7.3 Threat Intelligence and Awareness

National cyber threat assessments and reports enable consistent characterisation of cyber threats and risks and allow the identification of trends and changes in the activities of malicious actors, new vulnerabilities, or key technological developments impacting national resilience. Information about cyber incidents, threats, and vulnerabilities must be analysed and aggregated to provide timely and actionable information to government planning and decision-making entities.

Regular public threat notifications and reports, social media posts, and so on by, for example, the National Computer Security Incident Response Team (NCSIRT) the Computer Emergency Response Team (CERT), or another relevant authority support public threat awareness and inform the public about significant cyber incidents, major threats and/or vulnerabilities, and to give insight into trends. Such reports and notices may also alert the public to current cyberattack campaigns or systemic vulnerabilities. By sharing timely information, the Government can motivate organisations to work together to prevent cyber incidents and achieve safer cyberspace.

By the respective authority or team (CERT or NCSIRT) guidelines and tool recommendations for MDAs must be composed that allow MDAs to conduct vulnerability assessments at the very early stage of introducing new solutions to the public sector. The vulnerability assessments should include the following assessment types:

- **Host assessment:** This looks at critical servers that might be open to attacks if not tested properly or created from a secure machine image
- **Network and Wireless Assessment:** This checks policies and practices to stop unauthorized access to networks and resources
- **Database Assessment:** This reviews databases or big data systems for vulnerabilities and mistakes, finds insecure environments, and filters sensitive data.

Cooperation with the Zimbabwe Republic Police is critical for the threat intelligence functionality provider.

8 Security Architecture Artefacts

Typical Security Architecture Artefacts include:

- Legal acts or policy documents assigning responsibility for Cybersecurity.
- Methodology.
- Business rules regarding handling of data/information assets.
- Written and published security policy.
- Codified data/information asset ownership and custody.
- Risk analysis documentation.
- Data classification policy documentation.

The list of Artefacts and their content is suggested to be revisited and adjusted when changes in legal and technical, strategic and operational levels.

8.1 Policies

Cybersecurity as a complex domain takes a long time to establish necessary organisational and technical solutions for reliable operation while the ZWoGA is being implemented. However, due to the nature of security - one must always be ready to take care of new and changing threats - there is a need for a mechanism, that helps to communicate clear instructions on specific security fields. Security policies can be used as such instruments.

In the long-term policies should find a resolution in relevant regulation or security framework but there can be aspects where policy will remain the best tool for establishing clear rules on peculiar topics. Therefore, a list of security-related policies must be maintained and their relevance regularly reassessed.

During the first Architecture development iteration workshops the stakeholders expressed their priorities related to most critical policies in the ZWoGA. The results are presented in Table 27.

Table 27 Security-related policies to be developed as indicated by MDAs

Policy topic	Sum of Votes
Enterprise Architecture Policy	13
IT Governance Policy	9
Information Security Policy	5
Disaster Recovery and Business Continuity Policy	5

Policy topic	Sum of Votes
Password policy	2
Bring Your Own Device (BYOD)	2
Compliance and Regulatory Policy	1
Change Management Policy	1
Procurement and Vendor Management Policy	1
Business Process Management Policy	1
Interoperability Policy	1
Data Sharing and Collaboration Policy	1
Cybersecurity Incident Response Policy	0
Enterprise Data Architecture Policy	0
Disposal of IT gadgets	0
Training and Awareness Policy	0
Digital Identity Policy	0
Application Development and Maintenance Policy	0

The security-related policies, starting from the most critical must be developed, approved and adopted. It is suggested to select just a few of them in the beginning to be implemented and select the next set after that.

For the future, considering the technical security of information systems, the following security-affected policies should be considered also as high-priority policies:

- Accepted development methodologies and critical properties of development methodologies - providing necessary properties of development methodologies of each solution development project.
- Source code management - how the source code of all governmental executables is managed (including license management), validated, tested and availability ensured.

- Deployment instances and their usage - describes what staging instances and execution environments are used in alignment with general solution development methodology and CI/CD processes.
- Software quality insurance - describing the minimal set of tests that need to be included with every solution delivery.

8.2 Non-Functional Requirements

Non-functional requirements (NFR) focus on how the system performs its functions, they address aspects like scalability, performance, security, usability, reliability and maintainability.

The list of requirements/table to be fulfilled must include fields like type/category of requirement, unique/referential number, requirement, and comment. The NFR, fulfilled with the actual situation in the Comment field must be attached to every system and might be MDA-internal (not public).

The set of requirements is intended for use by

1) architects, product and project managers when designing software and procuring or receiving development works, and
2) for developers when fulfilling development contracts.

The requirements are formulated based on the long-term experience of development projects and highlight areas and issues that require special attention. Behind practically every claim, someone has encountered a problem. Based on experience, an attempt has been made to formulate an abstract rule. The purpose of the requirements is to prevent the recurrence of problems.

The NFR must be included in the procurement (or used as input for in-house developments) and compliance with all the requirements must be required (exceptions can be agreed upon when the owner of the requirement agrees to that).

When applying the requirements here, one must be flexible and consider the particularities of the specific software system. Requirements that cannot be met due to the specifics of the software system or are not reasonable to be met or are reasonable to be met partially or in a significantly different way, must be identified and their special treatment determined. Variations (non- or partial implementation, if it is practical) are allowed with the consent of the customer.

It must also be considered that the set of requirements is neither comprehensive nor complete. The NFR must be seen as the current best understanding of such requirements. When updating a system and the NFR has been updated then by default the changed NFR requirements must also be adapted to the system.

An example of security-related non-functional requirements continues.

Table 28 Non-Functional Requirements

Type / category	Reference Number	Requirement	Owner
Availability	1.1	New module deployment mustn't impact the front page, product pages, and checkout page availability and mustn't take longer than one hour. The rest of the pages that may experience problems must display a notification with a timer showing when the system is going to be up again.	(name and affiliation of the person who states the necessity of the requirements)
	1.2	The average system downtime per [period] is not more than [percentage].	
	1.3	In production environments, applications are automatically monitored.	
Interoperability	2.1	Applications are designed and developed following the principles of Domain Driven Design and Microservices Architecture.	
	2.2	Data exchange between information systems takes place over the [system].	
Performance	3.1	The front-page load time must be no more than [seconds] for users that access the website using mobile connection.	
Reliability	4.1	The database update process must roll back all related updates when any update fails.	
	4.2	The delivery of the application to the production environment is carried out on a blue-green basis, i.e. the operation of the service dependent on the application is not interrupted during the upgrade.	
	4.3	Planned downtimes of the system are informed in advance of [time].	

Type / category	Reference Number	Requirement	Owner
Security	5.1	The URL must not contain personal information or a session key.	
	5.2	The user interface and technical components communicate over TLS/SSL. It also required for intranet applications.	
	5.3	Keys, certificates, passwords and other sensitive information are not stored in a code repository or online documents. Use Vault-like solutions.	
	5.4	Access permissions for the [system] may only be changed by the system's data administrator.	
	5.5	Administrator access to the system is available only from intranet / specified IP.	
	5.6	Administrator and editor access must use MFA.	
Usability	6.1	People with no understanding of [language] must be able to use the product.	
	6.2	Keyboard users who navigate a website using <tab>, must be able to reach the [functionality] button from a product page in [count] <tab> clicks.	
	6.3	All governmental websites use the same design framework.	
Development	7.1	The application code is versioned using Git.	
	7.2	For database upgrades, there must be database migration scripts.	

Type / category	Reference Number	Requirement	Owner
	7.3	The source code is written with clarity, which allows a software developer with professional training to further develop the system.	
	7.4	Additional recommendation: Application source code and comments must be in [language].	
Deployment	8.1	The application must have passed security testing before going into production.	
	8.2	Vulnerability detection is manual or automated, for example because of code analysis.	
	8.3	Code that fails tests will not go into production.	
	8.4	An application will not go into a production environment if security weaknesses and/or vulnerabilities have been discovered. Excluded: If alternative compensatory measures have been implemented in the architecture and a risk assessment has been made for them.	
	8.5	The delivery of the application to the production environment is carried out on a blue-green basis, i.e. the operation of the service dependent on the application is not interrupted during the upgrade.	
Maintainability	9.1		
Portability	10.1		

Type / category	Reference Number	Requirement	Owner
Scalability	11.1	The website attendance limit must be scalable enough to support [users] at a time.	
Reusability	12.1		
License	13.1	Mark the application software with a license. The copyright of the work must be clearly stated.	
	13.2	Additional recommendation: Use the MIT license. An alternative is the EUPL.	
Data	14.1	Data must be stored in at least UTF-8 encoding.	
	14.2	A data description has been prepared for the information System.	

8.3 Critical Information Infrastructure and Vital Service Providers

Certain sectors and services are commonly recognised to be essential to the normal functioning of society, the economy, and the state. These typically include energy production and supply, communications, financial services, healthcare, utilities, and others.

A list of such service providers must be revised and published using specific regulations as the status comes with extended attention to the security of the information infrastructure.

Examples of services in strong relation to ICT and their proposed responsible MDAs are presented in the table below.

Table 29 Vital Service Providers

Type of Service	Responsible MDA	Service providers	Service details
Electricity supply	Zimbabwe Electricity Supply Authority (ZESA) and delegated subsidiaries	TBD	
Data service	NDC / TelOne / Utande internet services / ZimStat	TBD	
Mobile phone service	NetOne Cellular / Econet Wireless / Telecel	TBD	
Electronic identification	Ministry of Health / Zimbabwe Population Registration System (ZPRS)	TBD	
Authentication and digital signing	MICTPCS	TBD	

The type of services in other areas might include as following:

- Payment services.
- Cash circulation.
- District heating.
- Ensuring the drivability of the national road.
- Water supply and sewerage.
- Electricity supply.
- Natural gas supply.
- Liquid fuel supply.
- Telephone service.
- Provision of food and medicine.
- Healthcare service.
- Operation of airports.
- Air navigation service.
- Operation of the public railway.
- Operation of ports.

9 Organisational view

Organisational structure, as applied to the Security Architecture of ZWoGA, is a valuable and necessary management tool to organise tasks and people in an intelligent, meaningful, and responsible structure to meet and successfully discharge the security function in any country.

For implementing Security Architecture as an integral part of ZWoGA the following roles are needed in the Zimbabwean public sector:

- Government Chief Information Security Officer (GCISO),
- CISOs, technical / Cybersecurity architects of MDAs.

The Government Chief Information Security Officer (GCISO) role is responsible for the strategic direction and prioritisation of the GoZ's approach to information security. The GCISO draws on the technical expertise, relationships, and unique insights of both the Zimbabwe National CIRT (unit in POTRAZ) and the MICTPCS to uplift information security practice across the government.

Fulfilment of the role of GCISO might be included in the tasks of Cybersecurity and Monitoring of Interceptions of Communications Centre at OPC or into Chairperson of Cybersecurity Committee.

To ensure capacity building and a solid knowledge base of security architects, the human resourcing of MDAs with qualified cyber-security skilled personnel from different backgrounds is suggested with the help of the Ministry of Higher and Tertiary Education, Innovation, Science and Technology Development (MHTESTD) and/or Public Service Commission, (PSC). The students with cyber safety competencies available at Harare Institute of Technology, Information Security & Assurance might also be asked to participate as early as possible.

The result of such combination is explained in the artefact: Vision and Goal of ZWoGA (D4-1).

We also emphasize the need for supervision; it is suggested to promote regular auditing of existing and new ICT systems in Zimbabwe by members of ISACA Zimbabwe Chapter and/or security checks by Zimbabwe National CIRT (unit in POTRAZ).

10 Dependencies

Security Architecture does not exist per se, it has relation and impact to Legal, Foundational Projects/Enablers, Integrated Public Services (IPS), Applications, Technology and Data, Change Management and Communication as well.

Even if it is written as separate from other architecture documents, it is important to emphasize, that security by design, its building blocks, artefacts and policies collected here are at the same time integral parts of all other architectures as well, must be considered.

Therefore, it is important not to keep security aspects available only for GCISO and a small team of architects but to build trust and use it for communication between ICT of other (all) MDAs, together with private companies developing systems and citizens as end users of IPS.

Delivering a seamless Government experience

D5-1 Governance Architecture

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Table of Figures

List of Tables

1 Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the " An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for enterprise architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to enterprise architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

The current deliverable is oriented toward governing entities responsible for developing and implementing the first iteration of the Enterprise Architecture.

Architecture governance should be revised at the beginning of each architecture iteration, and relevant stakeholders (entities participating in the architecture governance) should be informed of their roles and responsibilities based on the structure suggested in this report.

The governance of architecture provides only artefacts, giving an overview of architectural governance and relevant parties. No building block concepts are defined in this domain, as the whole domain is more procedural.

2 Artefacts

2.1 Artefact: Governance Model

To ensure that the architecture work follows set goals/vision, and would be implemented by relevant stakeholders, a clear governance model with a clear command line needs to be in place. Additionally, the architecture development and implementation process should be engaging and ensure that experts with the agency would have a strong co-

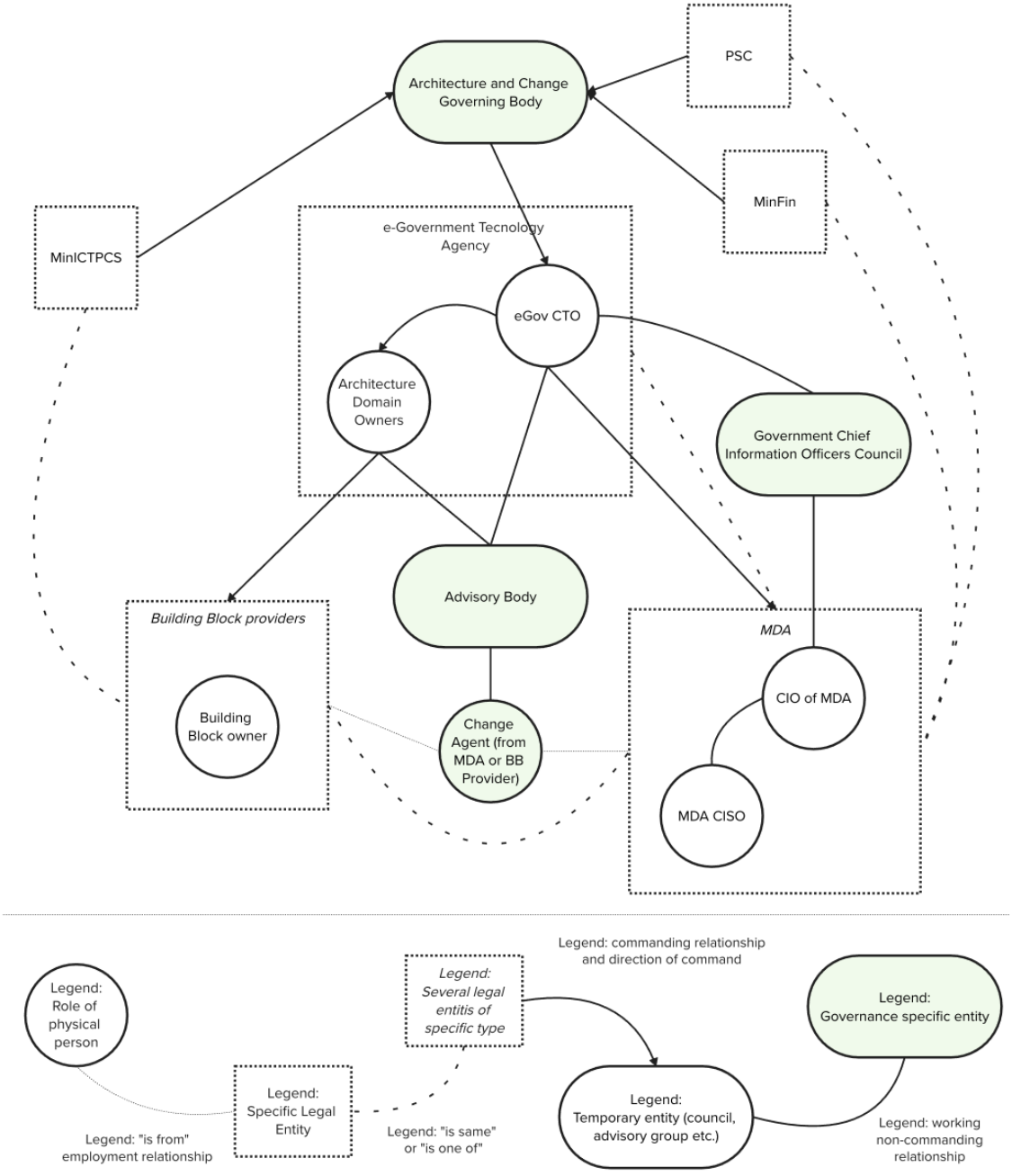


Figure 24 Governance Model

working environment – therefore, also semi- and non-formal relationships between stakeholders must be considered and exposed in the governance model.

The model presented in Figure 24 presents the governance model for the first iteration of the Enterprise Architecture.

The key aspects depicted in the model are the following:

1. Commanding relationships
    a. Architecture and Change Governing Body - while the e-Governance Technology Agency (EGTA) has its clear mandate in Zimbabwe, the ZWoGA governance requires the highest level of decision to be balanced by key stakeholders in the domain: besides the EGTA, the Ministry of Information and Communication Technology, Postal and Courier Services (MinICTPCS), the Ministry of Finance (MinFin), and the Public Service Commission (PSC) are expected to man the governing body with representatives and their organisational positions. The EGTA CTO, as operational lead for the activities, is responsible for the Governing body.
    b. The MDAs and entities with ownership of building blocks (from IPC, application, technology and data architecture) report to the EGTA CTO.
    c. For each architecture domain, the respective owner is the commanding officer for building block owners in the relevant architecture domain.
2. Non-command relationships
    a. The advisory group of key change agents supports the governance body—highly engaged experts from selected MDA. The Change Strategy clarifies the working relationship between change agents and the advisory board.
    b. Architecture domain owners have a working relationship with the Advisory Body (preferably a subset of the Advisory Body formed from Change Agents who have a specific interest in the respective architecture domain) for developing the domain architecture during the architecture development phase.
3. Additional relationships
    a. The CIO Council monitors the progress of changes and collects further requirements from MDAs.

Key responsibilities of participants in the governance model:

- Architecture and Change Governing Body - decision-making.
- CTO of EGTA - ensures that the change is managed, and the roadmap fulfilled. Monitors risk related to the architecture changes and implementation.

- Architecture Domain Owner - a person for each architecture domain (IPS, application, technology, data, security; for governance architecture the CTO of EGTA is the domain owner) who has the responsibility to arrange work during architecture development and steer work during the architecture implementation phase.
- Advisory body and change agents - communicates and engages stakeholders in the process and informs EGTA on challenges of engagement. Key facilitators of the change work.
- MDA - engage in the change process by sharing information on requirements and expectations and reporting on implementation progress and challenges.
- Building Block provider - follow instructions from the Governing Body and EGTA and ensure on-time readiness and operations of the relevant building blocks.
- CIO Council - advice EGTA CTO on operational and resource requirements to keep planning adequate.

The Advisory Body should be seen as the brain trust helping EGTA, Architecture Domain owners and Building Block owners to do the right thing. The Advisory Body should have enough participants that it would be able to:

- Split into sub-groups for specific architecture domain-specific developments (or preparing for following architecture development interactions).
- Communicate two ways with their affiliate MDA on the developments and the ideas discussed in the Advisory Group.

2.2 Artefact: Roles and Skills

Key positions in the governance model are expected to have some skills. While at the top level, some positions could be newly established then in general (especially in MDAs) the positions should be assigned to persons already in the organisations as it does not require a full-time load when participating in the architecture development and implementation.

The following table suggests key skills that are beneficial to persons identified in the governance model (see Figure 24 Governance Model).

Table 30 Roles and Skills

Role	Affiliation	Skills
eGov CTO	e-Government Technology Agency	• IT-management professional • Visionary, evangelism.
Architecture Domain Owner	e-Government Technology Agency	• Business architect

Role	Affiliation	Skills
		• Good knowledge of the domain the person is responsible for • Analytical • Leadership and engagement skills (for architecture development with Advisory Body)
Building block owner	OPC or MDA taking leader role and top management responsibility for a building block.	• Expert of specific domain • Comprehensive understanding of ICT-product/-service (ownership) • Communication skills (for building block existing and potential users).
CIO	MDAs	• Leadership skills • Strategic planning • Administrative skills (resource and HR planning, implementing) • Inter- and intra-organisational communication
CISO	MDAs	• IT-security management and/or expert • Risk communication
Change agent	Any entity	• Leadership and engagement skills • Opinion leader in respective field • Communication skills

2.3 Artefact: Governance and Communication Matrix

Communication between different actors in the Enterprise Architecture must rely on mutual agreements and consider the opinions of various stakeholders.

As the governance model for Enterprise Architecture suggests forming governance-specific entities, their main stakeholders (target audiences) and communication pathways are outlined below.

Although the governance structure is hierarchical, for cooperation, two-way communication channels are included as collaboration and getting feedback are crucial for the success of the Enterprise Architecture governance.

Table 31 Artefact: Communication

Entity	Main target audiences	Communication pathways
Architecture and Change Governing Body	MinICTPCS Ministry of Finance Public Service Commission	• Progress reports (milestones achieved, timelines met, etc. • Monthly updates (newsletters, e-mail lists) on the latest developments • Regular workshops to disseminate information and encourage knowledge sharing • Study trips to learn about best practices • White papers on the relevant topics to inform stakeholders and guide decision-making
Advisory Body	e-Government Technology Agency MDAs Building Block providers	• Roundtable meetings and discussions to exchange ideas and address challengers • Surveys to gather feedback from stakeholders on specific topics and their needs and priorities • Presentations to raise awareness about e-government initiatives and their benefits • Videos to promote change initiatives and enterprise architecture • Regular meetings with meeting notes published/e-mailed
Government Chief Information Officers Council	e-Government Technology Agency MDAs	• Working group reports to document outcomes and recommendations • Workshops, breakfast/lunch meetings to foster collaboration and information exchange among stakeholders • Surveys to assess the progress of initiatives within government entities • Results presentation to leadership teams • Social media posts to promote initiatives and achievements and gather feedback • Case studies to document successful e-government implementations • Data visualisations and infographics to communicate progress and impact
e-Government Technology Agency	PSC MinFin	• Annual conference to bring together wide range of stakeholders from public and private sector • Quarterly reports • Monthly updates (newsletters, e-mail lists)

Entity	Main target audiences	Communication pathways
	MinICTPCS MDAs Building Block providers	• Communication campaigns to raise awareness and understanding of e-government initiatives/EA developments • Competitions to incentivise the uptake of new building blocks or other initiatives related to Enterprise Architecture • Social media posts to promote e-government initiatives and engage with the public • Interviews and articles for success stories and expert insights on the implementation of the EA • Case studies to document successful e-Governance implementations • Data visualisations and infographics to communicate progress and impact • Study trips to learn about best practices • Surveys to gather feedback from the public on their needs and experiences related to e-government • Newsletter for EA topics

3 Dependencies

Governance architecture, as an oversight domain, is like all other architecture domains, including Security Architecture, Data Architecture, Integrated Public Service Architecture, Application Architecture, and Technology Architecture.

The governance architecture's role is to verify that their respective owners are handling architecture work and the implementation of building blocks.

If a decision inside architecture domains does not affect other domains, work in each architecture domain should be independent. However, if an adjustment and implementation impact other architecture domains, then such enhancement ideas and changes should be exposed to them by the means provided by the governance domain. Therefore, effective and constant cooperation and communication between parties are crucial.

Delivering a seamless Government experience

D5-2 Change Strategy

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

1 Executive Summary

This report presents practical guidance to navigate the change process in developing a Government Enterprise Architecture for the Government of Zimbabwe. It suggests governing structures and a roadmap to prepare, engage and empower people leading the change – the change agents. This report's findings and recommendations result from three on-site interviews and workshops. The structure and approach were extensively discussed and developed based on the change management workshop with key stakeholders from MDAs in Mutare on 8-10 May 2024.

The report was a collaborative effort developed by the experts of the e-Governance Academy – Kristi Kivilo, Randel Länts, Dr Kristina Reinsalu, and Rica Williams, with the kind support of Moffat Nyamadzawo.

The authors extend their gratitude to the dedicated participants from the Office of the President and Cabinet (OPC), the Ministry of ICT, Postal and Courier Services (MICTPCS), and representatives from all other ministries, departments, and agencies (MDAs). Their active involvement and contributions were instrumental in enriching this analysis with significant insights and perspectives.

2 Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the " An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for enterprise architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to enterprise architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

Change management is often needed to ensure continued survival or business relevance. Combining change management with the management of project work offers the best potential for delivering new results and capabilities, successfully embedding the change, and enabling the required benefits. The change management process links strategy with execution and deployment with the operation and the ultimate realisation of the expected benefits.

This concept is particularly relevant to Zimbabwean government institutions responsible for change when implementing the whole-of-government enterprise architecture and going through digital transformation at many layers. By integrating change management principles with project management practices, these institutions can better achieve their strategic goals and improve operational efficiency, enhancing public trust and institutional resilience.

3 Effective Change Management

3.1 Strategic Approach

Technology brings about significant changes in society. However, societal change, including technology, is tightly linked to people. While technology can be bought or developed, people delivering societal change must be inspired, engaged, and empowered. Thus, change management focuses on the social aspects (people side) of change.

In other words, it should provide a framework, set of tools, and approaches to enable an organisation to transform from an AS-IS state to the desired TO-BE situation. It is important to understand that change and its definition is a process of how an organisation will be changed, its impact and specific changes were seen across the organisation in behaviour, outputs, and outcomes (Cole, King, & Sowden, 2015).

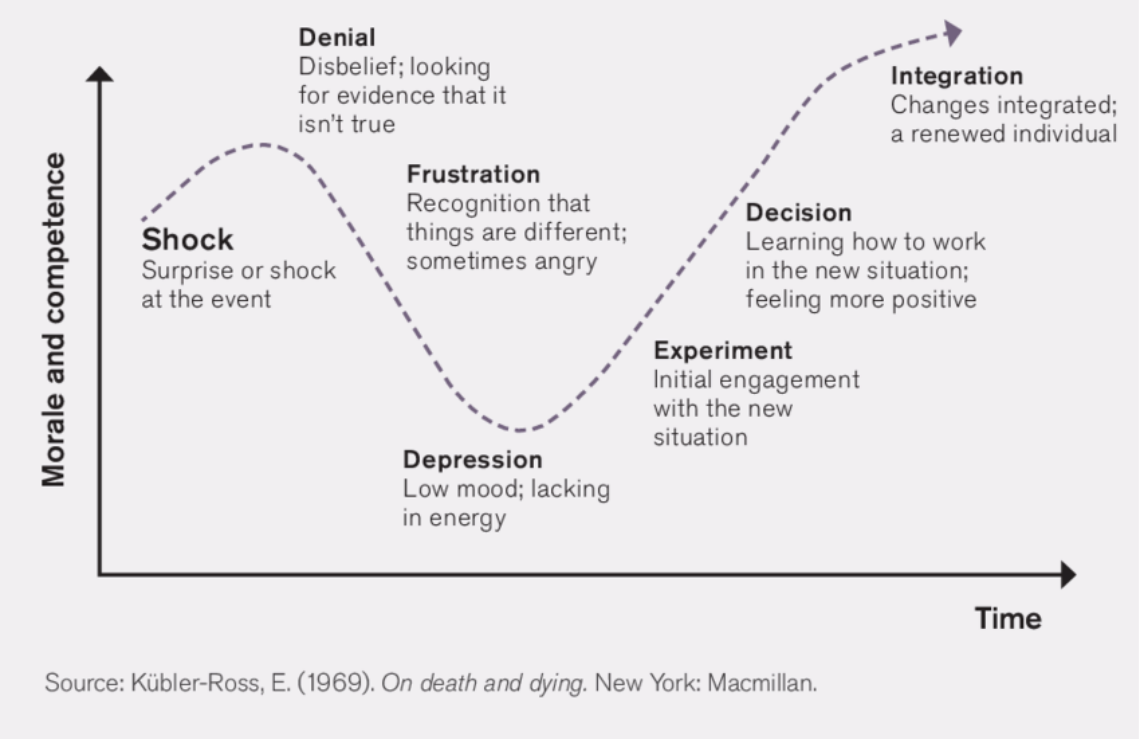


Figure 25 Change Acceptance

Change brings uncertainty and confusion. Change drags people out of their comfort zones and poses challenges. People often resist change for several reasons: fear of the unknown, lack of clarity, fear of losing a job, and lack of qualifications and skills. The concerns need to be addressed to overcome resistance.

Kübler-Ross graph explains the human response to change, where a change often comes as a shock followed by denial. Frustration and depression both relate to inner

resistance. However, if led and managed well, it will be followed by initially slow acceptance. It is critical to understand that leading a change, changing oneself and reaching the desired TO-BE state requires time. Change is never linear – there are pumps and setbacks along the way. In addition, change is constant – once the changes are integrated, usually the new change process begins.

The change curve is a function of time. Some apparent "resistance" simply reflects a difference between the position of those announcing a change and those receiving it. Those announcing the change have had a greater involvement in the process to this point, so their curve is shallower and shorter. They have also had more time to process the impact of change on themselves, so are typically further through the curve. At the point of announcement, those receiving the change are right at the start of their curve. (Smith, 2015, p. 11)

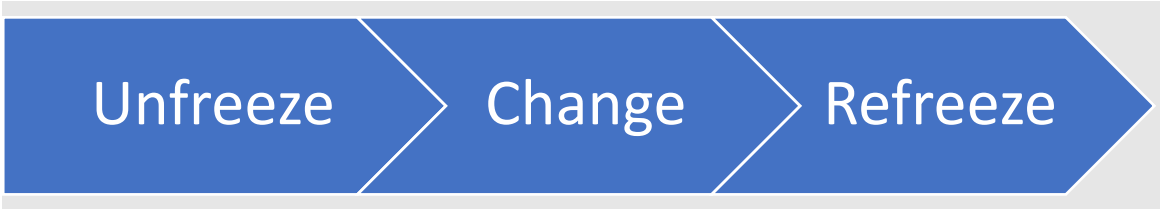


Figure 26 Lewin's Three-Step Approach

The **Unfreeze phase** includes three stages: defining the current situation, creating a vision, and identifying coalitions that drive and resist changes. In the **Change phase,** the involvement of people concerned is essential as is experimentation over solutions to problems. In the **Refreeze phase,** the new has settled and formed new knowledge, habits and working culture (Smith, 2015, pp. 36-37).

Kotter's model emphasizes effective leadership and should be treated as a roadmap to overcome typical errors in implementing the change (Kotter, 2012). The eight steps are the following (Smith, 2015, pp. 38-39):

1. **Establishing a sense of urgency** – identified sources of complacency and ways to raise the sense of urgency ("a majority of employees, perhaps 75 per cent of management overall, and virtually all top executives need to believe that considerable change is absolutely essential" (Kotter, 2012, p. 51)).
    - In the Government's Policy for ICT, it is noted that "the digital divide is widening between the '*digital haves*' and the '*digital have-nots*' and closing the gaps locally, nationally, and globally requires creative 'pro-people ICT Policies' that focus on national priorities, and on areas that will have a positive impact on people's lives" (Government of Zimbabwe, 2024). Thus, it is of utmost importance to close digital gaps so that the country can improve its socio-economic outlook, prosper, and become globally competitive.

2. **Creating the guiding coalition** – people with strong positional power, appropriate and varied expertise, credibility, and effective leadership.
    - The e-Government Unit in the OPC, in cooperation with MICTPCS, has played a pivotal role in engaging with MDAs across government structures and identifying key positions and people, forming a (loose) network of change agents – a coalition delivering change.
3. **Developing a vision and a strategy** – something that people can imagine, offering positive outcomes *("a picture of the future with some implicit or explicit commentary on why people should strive to create that future"* (Kotter, 2012, p. 71)).
    - The Zimbabwe National Vision states that Zimbabwe aims to attain an "upper-middle-income economy" status by 2030 (Government of Zimbabwe, 2022). Regarding ICT, the vision is to become "a knowledge-based society with ubiquitous connectivity by 2030 (Government of Zimbabwe, 2024).
4. **Communicating the change vision** – clear and direct language, using images and analogies, repeated, lived out by leaders.
    - While setting clear targets that are in line with the vision, use storytelling to make the task or path ahead easy to relate to. See more **Storytelling for Change Communication**.
5. **Empowering employees for board-based action** – providing systems and structures and appropriate training for employee action, removing or sidelining managers who might get in the way.
    - Defining roles within MDAs and setting up coordinated training and capacity-building programmes for civil servants to embrace the change, see more **Capacity Building Framework**.
6. **Generating short-term wins** – minimising negativity and uncertainty, promoting support, and recognising performing individuals.
    - Since the change is constant and complex, it is advisable to divide the process into parts or phases and to set achievable targets. This helps to keep people engaged and overcome change fatigue, see more Engagement and Minimising Change Fatigue.
    - During the change process, it is vital to assist those who are lagging and give more opportunities to provide and contribute to the people thriving in it. This allows us to extract more without leaving anyone behind.
7. **Consolidating gains and producing more change** – allocating more resources for more change and leadership.
    - Change is constant, and the government structure must always be fit to adapt and improve. Change is a continuous road, and when embarking on it, the journey itself becomes as important as reaching the destination.

8. **Anchoring new approaches in the culture** – aligning and promoting the new organisational culture (doing things in a new way and not falling back to the old).
    - There is often strong resistance to change, but if you keep old routines, you do not see the benefits. Therefore, it is particularly important to clearly show which old routines have become obstacles to change and address them. Being part of a change initiative can enhance the new culture within the public sector towards change and, more specifically, the use of the whole-of-government architecture.

3.2 Understanding Change

Key questions to consider when implementing change are:

- What is the change initiative?
- What is the process going to look like?
- What are the benefits?
- What are the roles?

As Rosabeth Moss Kanter outlines, the Ten Reasons People Resist Change provides valuable insights into the psychological and emotional factors that can hinder successful change initiatives. These reasons include:

1. **Loss of control**: Change can make individuals feel like they have lost control over their territory, leading to resistance. Leaders should involve those affected by change in decision-making to give them a sense of ownership.
2. **Excess uncertainty**: Change that feels like walking into the unknown can be met with resistance. Leaders should provide safety and an inspiring vision to overcome inertia.
3. **Surprise**: Sudden decisions imposed on people without time to prepare can be met with resistance. Leaders should avoid secrecy and instead plant seeds of change, seeking input.
4. **Everything seems different**: Too many unrelated differences a central change introduces can be distracting or confusing. Leaders should minimise unrelated changes and keep things familiar where possible.
5. **Loss of face**: Change often involves departing from the past, making those associated with the previous version defensive. Leaders should celebrate elements of the past worth honouring while making it clear that the world has changed.
6. **Concerns about competence**: Change can make individuals worry about their skills becoming obsolete. Leaders should provide reassurance through information, education, training, and support systems.

7. **More work**: Change often requires additional effort, which can be overwhelming. Leaders should acknowledge the demanding work of change and provide rewards and recognition to participants.
8. **Ripple effects**: Change can disrupt other departments, customers, and stakeholders, leading to resistance. Leaders should consider all affected parties and work with them to minimise disruption.
9. **Past resentments**: Previous negative experiences can resurface and hinder acceptance of change. Leaders should address past wounds and demonstrate that the world has changed.
10. **Real threats**: Change that poses significant threats, such as job losses or price cuts, can be met with resistance. To minimise discomfort, leaders should be honest, transparent, fast, and fair in their communication.

Ten reasons people resist change (Rosebeth Moss Kanter – Harvard Business Review 2012).

Understanding these reasons for resistance can help leaders anticipate and address potential barriers to change, increasing the likelihood of successful implementation.

Figure 27 What change means to me? Change management workshop

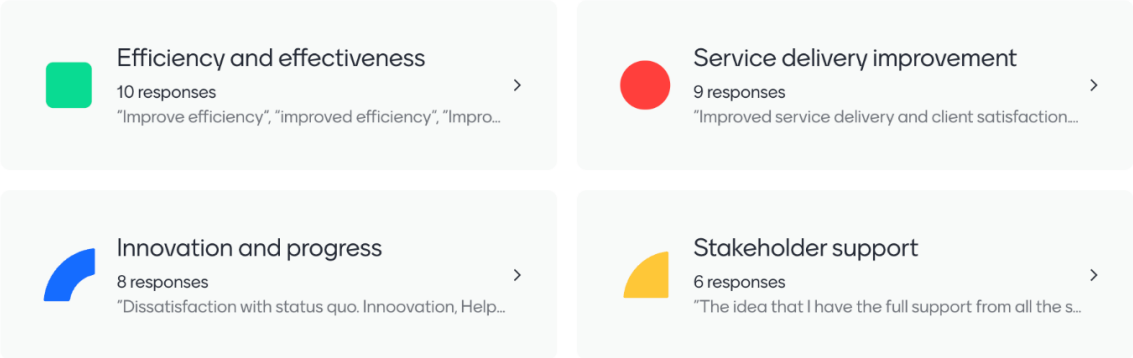


Figure 28 The motivation of change agents? change management workshop

3.3 Engagement and Minimising Change Fatigue

Representatives from MDAs across the government are integral to the desired change. Engaging stakeholders from an early phase increases the feeling of ownership. The workshops conducted served several purposes:

1. Creating a relaxed working atmosphere
2. Facilitating interaction between MDAs
3. Being an example of how to break the silo mentality
4. Using allocated time efficiently
5. Extracting maximum value from participants
6. Co-creating the uniquely Zimbabwean whole of government enterprise architecture

The collaborative method has two complementary values: emotional value and functional value. Emotional value motivates participants as they are asked to contribute. It inspires, as discussing with peers often opens new dimensions and perspectives. By sharing information and practices, it paves the way for innovation. Creating a relaxed and trusted environment builds trust, especially when formal positions are left aside, and the focus is on individual and collective contribution. This all forms the basis of a network (of change agents).

Functional value derives from the perspective of efficiency. It informs and simplifies, as topics can be raised, and questions answered in a group or work collectively rather than individually. Simply bringing people together in a room connects them physically or emotionally by providing a platform for interaction. All these lead to saving costs and time.

3.4 Measuring Progress and Minimising Change Fatigue

When embarking on the journey of change, the destination often seems far away and abstract. To be able to evaluate the process – short-term goals, long-term goals, and

the main KPIs (key performance indicators) should be defined and agreed on: What is the baseline for how things currently stand? What is the timeline for measuring the progress, and how will success be measured? What is the endpoint? How it will be measured and communicated?

We usually start by setting strategic objectives. These objectives are both the fundamental cornerstones and the desired outcomes. Whatever we are doing along the way, we must never lose sight of the objective.

However, these objectives are often abstract and to reach them, a clear strategy must be drafted and implemented. To ensure that our activities and plans are implemented, they should be divided into smaller parts and achievable goals. We should also be able to monitor and measure the progress.

The eGA experts reiterated the need to start with small and tangible goals. eGA, together with the OPC is working on foundational projects – integral parts of the whole of government enterprise architecture – that are small enough to be delivered quickly. Such projects help us to make and demonstrate progress, celebrate achievement, keep people (stakeholders, MDAs) motivated and, thus, overcome the potential fatigue caused by lack of so-called low-hanging fruits.

4 Governance and Stakeholders

In the workshops conducted in Mutare, different roles in MDAs were discussed. We used the following division of roles in a changing organisation (or in a whole-of-government structure) (Smith, 2015, pp. 50-51):

- **Idea generator** – develops and promotes ideas,
- **Sponsor** – executive leader with formal authority; enabler; addresses barriers; supports change; spokesperson,
- **Line management** – leader or manager at MDA level,
- **Targets** – implementers; people who need to change,
- **Change agents** – no formal authority; informal, inspirational leaders; change facilitators.

Roles are either defined by organisational structures or based on personal characteristics. The first should be seen as a hierarchical, subordinating system of an organisation where roles and responsibilities are linked to a position. Personal characteristics often determine what roles and responsibilities people take themselves within a group or working environment. Both are equally important. The organisational structure of government and MDAs is based on legal documents, thus providing a legislative framework, and a right to carry out duties. While roles based on personal characteristics – an agency – drive people from within.

For a successful implementation of change, one needs the right organisational structures and empowerment of agents.

4.1 Governance Structure

In the **Situation Analyses**, the following was stated:

> *Digital governance requires a designated institution with decision-making authority across the administration. While regional solutions are viable, coordination is essential, not to centralise but to align decisions. This institution's strategic role in building digital governance is crucial, with higher positioning improving directive power, its authority should be legislatively defined.*
>
> *Concerning the organisational structure for the establishment of digital government in Zimbabwe, …, the e-Government Unit situated within the OPC holds the responsibility for orchestrating coordination efforts, while MICTPCS is charged with the development of digital government infrastructure…*

The **Memorandum of Principles for the e-Government Act**, shared with eGA consultants, states that "e-Government presupposes governance and e-Government legislation therefore forms the basis of the governance framework" and foresees:

- Establishment of the e-Government Technology Agency and its roles including the e-Government Chief Technology Officer (EGTO) and Projects Management Office
- Establishment of an ICT Management Unit in each MDA headed by an MDA Chief Information Officer
- Establishment of Government Chief Information Officer's Council headed by the EGTO.

Problems identified during workshops:

- silo mentality – MDAs developing their online service with limited co-ordination
- lack of buy-in both above (politicians) and below (civil servants) – unclarity over the enterprise architecture, its need
- change resistance – fear of the unknown, see above.

4.2 Model

During the workshops and other events on change management, eGA committed to providing a governance structure or frame and a roadmap. As said above, to successfully implement changes in an organisation, formal structures must be filled or otherwise combined with people within the agency – change agents.

It is vital to clearly define and agree on ownership of the project. OPC has thus far taken the leading role. However, during our engagement activities, eGA experts have witnessed resistance to both the enterprise architecture exercise itself and OPC's role in it. It is vital to reach clarity on who is doing and is responsible for what.

eGA sees the e-Government Technology Unit situated within the OPC being given the co-ordinating role and echoes such proposal in the principles described above. The e-Government Technology Unit's role and responsibilities must be enshrined in decisions or legislative acts. That will enable the Unit to operate in a legal framework that is

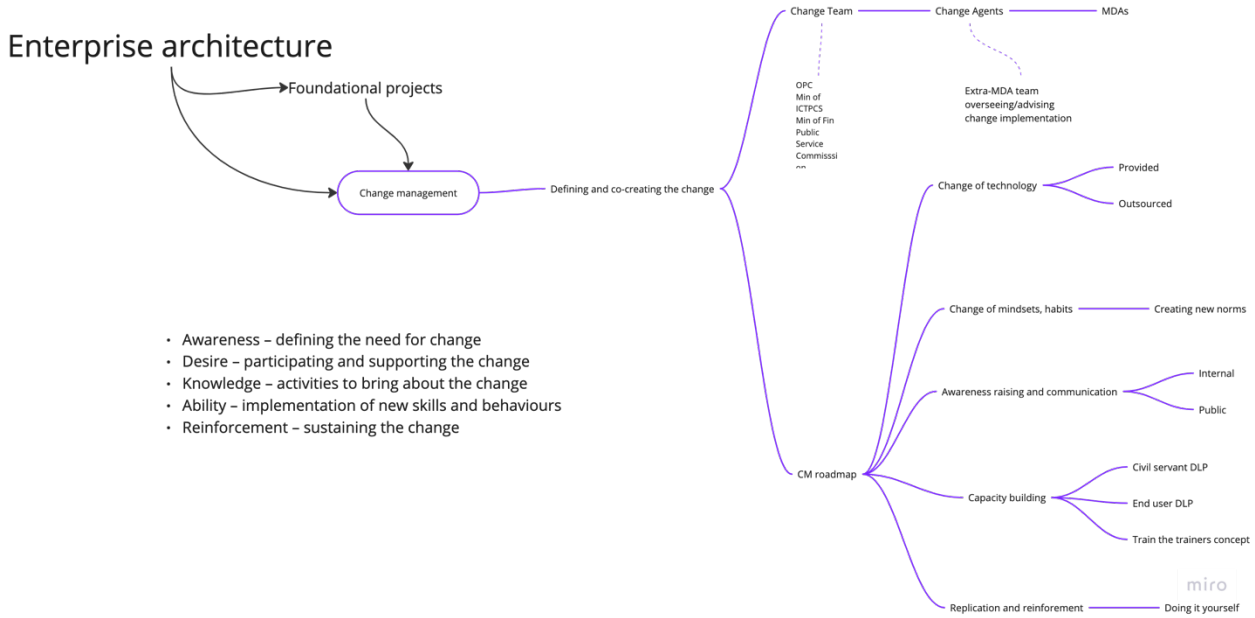


Figure 29 Change Management Governance Model

understood and accepted by other government institutions and bodies. However, eGA strongly encourages to not only limit the composition of the overseeing body – the e-Government Technology Unit – to solely OPC staff but to include key members from MDAs relevant for change implementation. eGA sees the inclusion of representatives of MICTPCS, PSC, and the Ministry of Finance as highly valuable, and thus recommends doing so.

Additionally, eGA suggests forming an advising body for the e-Government Technology Unit composed of change agents from MDAs to smoothen the change by bringing in an extra view from "the filed." Such an advisory body should be composed of people with either formal positions or agencies providing vital value to the governance model. It is worth mentioning that it must not necessarily include a member from each MDA, on the contrary, the advisory body must be small enough to be operational. However, again, the composition must be clearly defined, understood, and accepted by all.

5 Communication

5.1 Strategic Approach

As change always involves people, communicating is critical for change initiatives to be successful. To a larger or smaller extent, people who are impacted by changes need to be prepared to accept the change and adopt new ways of thinking or behaviours.

Throughout the change initiatives, anxiety and fear levels can be high because of fear of the unknown. In addition, different stakeholders might have their agendas and perceptions – this volatile environment around any large-scale change initiatives emphasises the need for strategic communication.

The objectives for the change communication plan are in correlation with the objective of the change – the change management team, therefore, must involve and work closely together with communication experts throughout the change initiative – from planning the change to evaluating its impact.

So, for example, if the objective for change in Enterprise Architecture is "80% of MDAs implement new Enterprise Architecture by 2028", then the communication objective would be "100% of the MDAs need to be aware of the new Enterprise Architecture by 2027".

A more specialised communication plan must accompany the change management plan to achieve any overall communication objective.

Change communication aims to set guidelines for strategic and effective communication with audiences (stakeholders) who are affected by the process, system and structural changes created by the enterprise architecture.

Communication activities fit on a scale from informing about the change (letting stakeholders know what, why and how the change is happening) to being engaged in the change (stakeholders are part of deciding what changes happen and how the changes are conducted).

Principles for effective communication

Communication activities – regardless of whether implemented by a specialist communication team, a change agent or other official – should follow the same principles.

Communication about the change initiative should be:

- **Accessible** – effective communication channels (for example, if the target audience does not use Facebook, it is not an effective channel), accessibility ensured (for example, information available in many languages if needed by target audiences, technological accessibility – text size, colours and contrast considered by following WCAG guidelines).

- **Relevant** – messaging should consider local context and be tailored to the specific communication needs of the target audience.
- **Beneficial** – include messages related to the specific benefits to overcome barriers and accept change, specific benefits to users.
- **Actionable** – most communication involves specific actions that target audiences need to take. These calls to action should be clear and easy to follow. For example – read more about the change from a link that refers them to a presentation and add a change management workshop to the calendar.
- **Timely** – timing messaging in a structured method. For example, expectations for change initiative timelines should be clear and any delays must be communicated quickly.
- **Credible** – using experts in the field helps to explain the reason behind the change and can help craft messages that address roadblocks and questions from target audiences.
- **Easy to understand** – when communicating technological change, simple language, effective visuals, and relatable stories help to communicate complex technological issues.

For change initiatives, all three levels of communication levels – from raising awareness about the change, supporting people affected by increasing their knowledge and helping to change their behaviour. The last two are linked to the capacity-building efforts related to change initiatives.

Figure 30 Communication Levels

A change initiative for Enterprise Architecture involves behaviour change for implementing new technological enablers or using new technologies or processes. For behaviour change more complex model needs to be implemented for communication. The behaviour change communication can be based on the internationally acknowledged and used COM-B model.

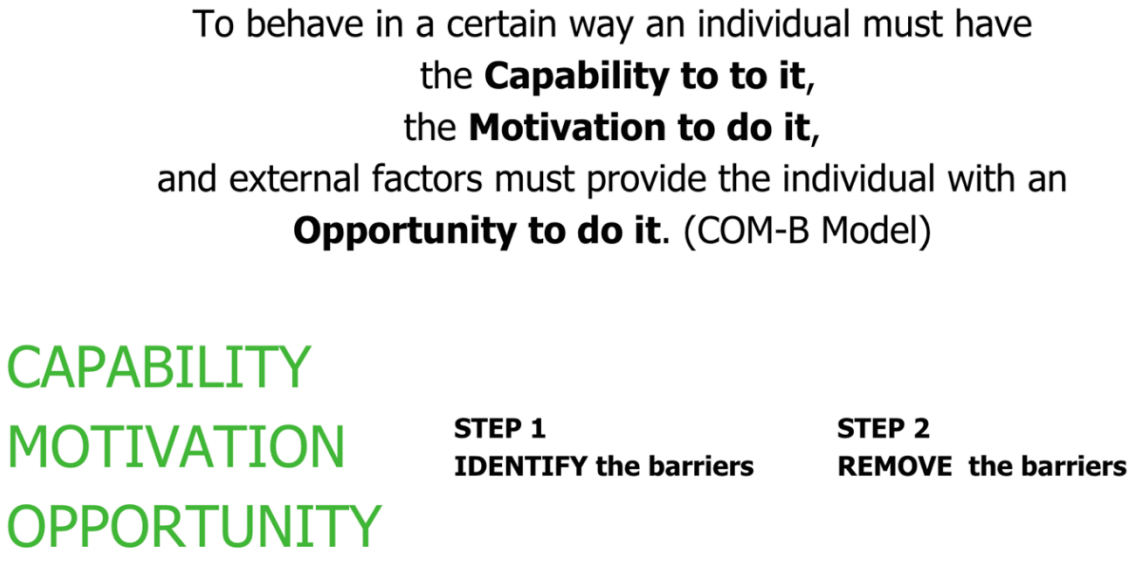


Figure 31 COM-B Model

Using the COM-B[1] model helps to "package" messages that create a behaviour change – adopting the change. And it is also useful for other interventions and activities to consider. For example, when designing interventions for people to learn digital skills or start using digital services, for employees to start using a new digital tool and so on.

1. There must be "capability" to do it: the people or people concerned must have the physical strength, knowledge, skills, stamina, etc to perform the behaviour. The capabilities can be divided into psychological and physical capabilities.

For example: To facilitate change related to the Enterprise Architecture it is crucial to ensure that individuals have the necessary capability – through training, coaching, and providing appropriate resources.

2. There must be the "opportunity" for the behaviour to occur in terms of a conducive physical and social environment: e.g. it must be physically accessible, affordable, and socially acceptable and there must be sufficient time. The opportunity is an external factor that needs to be present and can be divided into physical opportunity and social opportunity. The physical opportunity includes environmental and situational factors, such

[1] Source: UK Civil Service https://gcs.civilservice.gov.uk/wp-content/uploads/2021/02/The_principles_of_behaviour_change_communications.pdf

as infrastructure and physical barriers. The social opportunity includes cultural norms, social cues, and interpersonal influences.

For example, for the changes related to Enterprise architecture, the physical opportunity examples include having an internet connection and having the devices and software needed. The social examples include how change is perceived in the public sector, if there have been similar initiatives before, if is there trust in the leaders and so on.

3. There must be sufficient strong "motivation": i.e. they must be more highly motivated to do the behaviour at the relevant time than not to do the behaviour, or to engage in a competing behaviour. Motivation is the driving force that energizes and directs behaviour[2]. The motivation can be reflective or automatic. Reflective motivation includes conscious decision-making processes, such as beliefs, attitudes, and intentions. Automatic motivation is the emotional responses, habits, and impulses. Addressing the reflective and automatic motivations is crucial for fostering behaviour change and overcoming resistance.

For example, when Enterprise Architecture changes are being introduced, the reflective motivation can come from participating in specific change management workshops or Enterprise Architecture workshops. The automatic motivation can show in the initial reaction to proposed changes based on the culture within the public sector.

These components are interlinked – for example, increasing opportunity or capability can increase motivation and in turn, increased motivation can lead people to do things that will increase their capability or opportunity by changing behaviour.

[2] behaviourchangenetwork.com

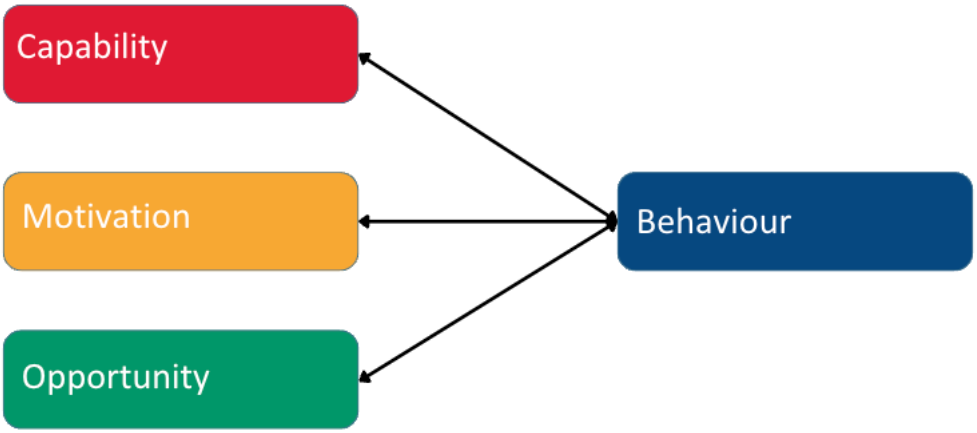


Figure 32 The Behaviour Change Wheel – A Guide to Designing Interventions

Figure 32 The Behaviour Change Wheel – A Guide to Designing Interventions presents the model by S. Michie, L. Atkins and R. West.

For example, technology-related changes need additional support to help people through the technological changes. Having the technology available is not enough. Having the technology is the opportunity aspect of the COM-B model, but for behaviour change also motivation and capability need to be addressed. Therefore, critical aspects such as understanding the technology and the change it brings need to be addressed. The benefits of the technology need to be clearly stated (from the audience's point of view) to increase motivation. Including engagement and feedback, opportunities can also increase motivation. And of course, for capability, several actions can be taken from awareness-raising activities to masterclasses, workshops, and seminars to e-learning.

For example, based on the COM-B model introducing a new IT system also needs:

- **Capability:** Comprehensive training programs, hands-on practice sessions, and simulations are developed and implemented.
- **Opportunity:** Required hardware, software, and technical support are readily available; helpdesk is established for the implementation phase; a positive work environment where colleagues can collaborate and learn from each other is fostered.
- **Motivation:** Benefits of the new system are communicated (improved efficiency and so on); employees are involved in the implementation process; employees who embrace change and contribute to it are recognised and rewarded.

The strategic communication that sets clear objectives follows effective communication principles and the COM-B model helps to communicate change to different audiences: within MDAs, between MDAs and other relevant organisations, civil servants, organisations, businesses, and members of the public affected by the interoperability framework and influence behaviours to adopt the changes and use technology.

Role of the Change Communicator

Change communicators are often required to be part of the change management team or steering group, helping to guide or take responsibility for the communication work stream.

The tasks of the change communicator include:

- identifying stakeholders and target audience members,
- developing communication objectives to support the transition,
- deciding the communication strategy and approach,
- crafting messages and other communication content,
- selecting communication channels,
- involving stakeholders and engaging them in the process,
- gathering and assessing feedback,
- measuring and evaluating success.

5.2 Messages and Channels

Crafting messages that support the change is one cornerstone of good communication. The messages must be relevant to target audiences – they stimulate awareness and understanding, enhance dialogues and so on.

Messages are not just brief sentences. Key points can be expanded, explained, and supported in diverse ways and through written visual and oral communication tools. The main messages must be aligned with the project's objectives and goals and tailored to the needs and interests of the target audience.

The simple principles to follow when creating messages are:

- keep them short and on the point,
- use clear and simple language,
- avoid jargon and acronyms,
- provide examples and be specific,
- Each message should include a fundamental statement (the one thing that you want the audience to know). That should be backed up by adding two to four support points, including data that is easy to understand.
- Use consistent tone and style when talking about the project.

Even within a large change initiative, there should be a limited number of messages. In one communication material up to three messages should be included. Message overload will contribute to the reader losing their focus.

For example, for Enterprise Architecture one possible key message could be:

"The whole-of-government Enterprise Architecture helps the public sector to provide better digital services for the citizens."

"Using the building blocks, such as integrated public service architecture, data architecture and security architecture the MDA's can create public services using already existing data."

"Using the service guidelines provided by Enterprise Architecture the citizens are provided with user-friendly services that help them save time and money. "

For communicating change the messages (and other communication means) need to cover some additional aspects:

1. Making sure everyone is aware of the change.
2. Explain the reasons for the change.
3. Get people on board with the change.
4. Minimise disruption caused by the change.
5. Address any concerns people may have about the change.
6. Provide information on how the change will be implemented.

Usually, communication channels are established within the public sector. But for change communication, it is useful to map them out again to choose a wider range of channels than used for regular communication such as announcements about policies or state visits and so on.

Classically, communication channels can be divided into:

1. For one-way communication: newsletter, e-mail, intranet, printed and digital materials (posters, flyers, yearbook, reports, video), public notices (formal announcements), blueprints, handbooks, special website and so on.
2. For two-way communication: group meetings, phone calls, focus groups, one-to-one meetings, conferences, away days etc, social media posts, press conferences, events, forums, WhatsApp groups and so on.

In addition to the classical channels used, there are examples of less-used channels and methods that can support change.

For example, for aspects of the Enterprise Architecture, there could be a competition to name new information systems or competitions for most active users, prices for feedback after the testing phase and so on.

5.3 Social Media

Although **social media communication should follow the same principles set out in the strategic approach, some aspects of communication should be highlighted when using social media.**

Social media helps promote e-government initiatives and encourage citizen engagement.

The main platform is Facebook for communicating with citizens. LinkedIn and Twitter should be used to share information with corporate and international stakeholders. YouTube channels can also be considered.

For social media content:

- Highlighting benefits - using understandable language to highlight how e-government solutions and e-services save time, improve efficiency, and increase transparency.
- Focusing on stories: Sharing real-life examples of citizens using e-services.
- Addressing concerns: Openly and proactively addressing concerns about digital security and data privacy.
- Using a multilingual approach: Where possible, including content in local languages to reach a wider audience.

Social media helps to create better engagement between the government and the citizens.

- Two-way communication: Responding to comments and questions promptly will encourage dialogue.
- Interactive content: Utilise polls and quizzes to increase engagement and gather user feedback.
- Partnering with influencers: Collaborating with trusted voices in Zimbabwe's online communities to amplify reach and build trust.
- Run targeted campaigns: Utilising social media advertising tools to reach specific demographics and locations.

The overall tone in social media should be:

- Informative: Providing clear and easy-to-understand information about digitalisation topics and e-services.

- Approachable: Using a friendly and welcoming tone that encourages citizens to explore e-government options.
- Empowering: Showing that e-government is a tool that empowers citizens to participate actively in government processes.

Hashtags

Hashtags for communication in Zimbabwe's digital transformation activities can leverage a two-tiered structure to maximize reach and engagement. The first tier could be a central country-related hashtag, like **#DigitalZimbabwe**, **#ZimGoesDigital**, or **#ZimDigital** This core hashtag would be used consistently across all communications to build brand recognition.

The second tier would incorporate more specific hashtags focused on program components or target audiences. For instance, **#FintechZimbabwe** could target the financial technology aspect, while **#eLearningZimbabwe** could address the education sector's digital transformation. A more general **#eGovernmentZimbabwe** can refer to topics related to e-Governance, **and #eServicesZimbabwe** for promoting new digital services. This dual approach ensures visibility and the ability to connect with distinct user groups within the larger initiative.

A slogan can also be used as a hashtag, for example, **#WeAreTheChange** to represent the vision for using technology to benefit the citizens.

5.4 Stakeholders and Their Impact

Analysing stakeholders helps to create tailored messages and communication mixes to support the process of change.

For most change initiatives, it is more impactful to segment the audiences to craft specific messages focusing on the audiences who are most directly affected by the change. The segmentation ensures that the stakeholders receive the information they need in a way that is relevant to their roles and interests. This leads to better buy-in and support for the proposed new whole-of-government Enterprise Architecture.

Stakeholders related to the new Enterprise Architecture change initiative can be categorised in a variety of ways.

1. By role: Management, IT leaders (CIO, CTO), Head of Departments etc.
2. By impact: **decision-makers** (who have THE authority to approve or reject the EA or its components), **implementers** (the organisations and teams responsible for developing the components of the EA or deploying solutions aligned with the EA and **end-users** (civil servants directly using the systems and processes defined by the EA). Also, the stakeholders can be divided on a high-low scale based on the impact they have from the change initiative: **Highly Impacted:**

This group directly experiences the biggest changes due to the policy. They might need more in-depth information and support during the transition. For example, departments responsible for implementing the policy, and public sector workers whose roles are significantly affected. **Moderately Impacted:** This group experiences some impact but might require less detailed information. For example: Departments that collaborate or interact with the affected departments, public sector workers whose roles are indirectly affected. **Low Impact:** This group experiences minimal changes but should still be informed. For example: The public sector workforce. Departments that are not directly connected to the policy area.

3. Level of detail needed: from the high-level audience who needs an overview and key principles for the new EA; a mid-level audience who requires more detailed information about the specific areas or components of the EA (for example, data, digital services, digital ID) to a technical audience who needs in-depth technical specifications and blueprints.
4. Resistance vs support: identifying the stakeholders who might resist the changes proposed by the new Enterprise Architecture and tailoring the communication accordingly.

A power vs influence matrix can be used to define communication goals for specific stakeholders.

Figure 33 The Power/Interest matrix

For communication purposes, it is vital to mark that stakeholders with high influence and high interest in the issue need to be engaged the most as their opinions and actions

can influence the course of the change initiative. This also means more effort to communicate with them should be made. High-power but low-interest stakeholders can become a threat if they do not understand the issue; therefore, communicating the vision and principles of the change initiative is vital. Low-power and low-interest stakeholders still need to be informed but should not be overwhelmed with information. High-interest but low-influence stakeholders can be seen as advocates on the ground and can bring back valuable feedback about the change initiative.

The process of introducing the whole-of-government Enterprise Architecture involves many stakeholders. Therefore, it is important to prioritise the stakeholders based on their influence and involvement. Also, for each larger part of the Enterprise Architecture, a more specific stakeholder mapping should be carried out. The most important stakeholders are therefore the OPC and MDAs. These stakeholders represent the organisational environment. The communication for implementing Enterprise Architecture involves:

1. Internal communication within the MDAs and other stakeholders to increase awareness about the change, activate change agents within the organisation and so on.
2. Inter-organisational communication – establishing communication channels and pathways between organisations to engage with other stakeholders, find better solutions, and create understanding and uptake for the change. The main communication challenge here is overcoming barriers and increasing cooperation.
3. Crisis communication – as any change has always been an element of jeopardy crisis communication needs to be planned from the beginning – especially when implementing large-scale IT systems or ID-systems.

Although the initial focus for change communication should be on the organisations most involved and affected, at later stages of the change management the stakeholders from the connected environment – the stakeholders that the MDAs need to build and maintain relationships with. These involve of course the customers (the citizens), developers, other organisations offering the service and so on. The last group of stakeholders belong to the wider influence area. These are stakeholders that can affect how the changes are perceived and implemented. For example, there could be economic changes or policy changes from international organisations and so on.

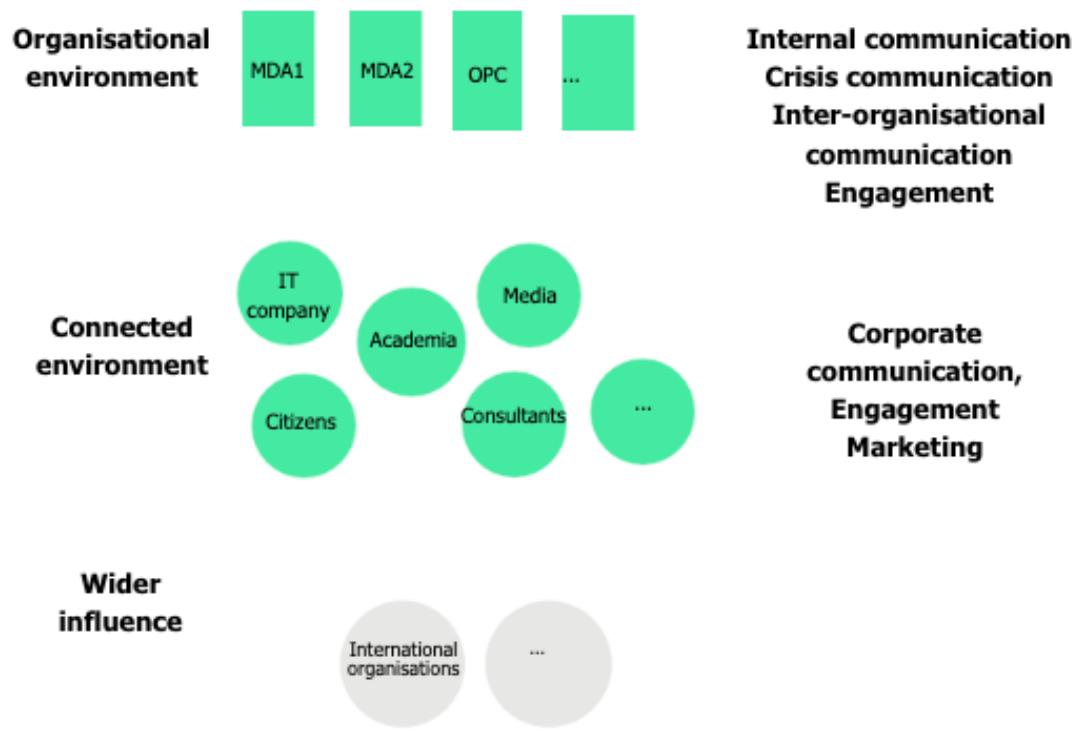


Figure 34 Communication Environments

Examples of communication activities for stakeholder levels are presented below.

At the policy level: Decision-makers engaged.

- Changes to regulations made.
- Information is available with explanations and implications for target groups.

At the institutional level: Stakeholder engagement and communication, internal communication

- Regular cooperation circle between the public and private sector
- Seminars, training programs, information days
- Working groups
- Presentations, animations, videos
- Stakeholder surveys
- News in the media, interviews, articles, and blogs
- FAQ on the website
- Contacts for different topics are easy to find on the website.

At the individual level: key individuals engaged.

- Participating in workshops, seminars events relevant to the topic.

- One-on-one meetings with key individuals – all levels from leadership to IT specialists.
- One-on-one customer support.

The areas that messages need to address:

1. Context and rationale – why are the changes happening, and what factors caused them? Focusing on "what does it mean to me?" (from the point of view of the stakeholders)
2. Vision for the future – what will the future look like, and how it will be different and better? What are the milestones, and when something is going to happen?

5.5 Storytelling for Change Communication

Successful communication and engagement should also consider people's emotional side, not just the rational side. So, in addition to logical reasoning to explain the change appealing to the emotions is also necessary. This can be done via storytelling, using symbols and metaphors. As Enterprise Architecture is designed to consider the specific needs and challenges in Zimbabwe, the language used in communicating it (for wide-level messaging – talking about the vision and benefits) can also use uniquely Zimbabwean concepts. Telling stories with Zimbabwean symbols and cultural concepts can help build a bridge between the technical nature of the topic and the true benefit of it to the Zimbabwean people.

The vision of (WoGA) defines the expected future state and long-term aspirations for the government that empowers ICT, what the government wants to achieve through ICT and serves as a guideline for managing and leveraging ICT resources and decisions. The (ZWoGA) goal agreed by MDAs is:

Providing a strategic framework for aligning and integrating government ICT infrastructure and systems.

Motos for change agents to emphasise the benefits anyone involved in the EA process can have on society (motivation for COM-B):

We are the people to make the change impactful

We are the change that will directly benefit our citizens

There can be many examples of known symbols and values to Zimbabweans that relate to Enterprise Architecture. For example:

- **The Great Dyke** – We are exploring technologies to uncover the potential riches for our citizens.
- **Balancing rocks** symbolising resilience, stability, unity, and diversity in managing change and utilizing the whole of government enterprise architecture.
- **A baobab tree** – small systems growing into one well-functioning ecosystem.
- The concept of ubuntu – finding consensus in topics and caring for everyone.
- **Colours of the flag –** for implementing Enterprise architecture effort (red), resources (yellow), discussion (white), ownership (black) and benefits (green) need to be addressed.
- Despite **speaking 16 different languages**, we speak the same language in terms of creating a better life for our citizens thanks to the more effective processes and to the whole of government architecture.

These are just some of the examples that can be used to rely on the vision behind the whole-of-government Enterprise Architecture.

6 Capacity-building and Skills

6.1 Strategic Approach

Digital skill proficiency is essential for successful digital transformation in societies and public administrations. Digital skills allow both the adoption of essential technologies and the adaptation to new ones.

Digital transformation and connected projects are about removing outdated processes, services, and legacy technology and planning and building data-based, user-centric, secure, and user-centric cyber services with modern technologies. Digital transformation is also about working differently; for this reason, digital transformation is tightly linked to human resources and needs a capacity-building focus for all those involved in the digital transformation process.

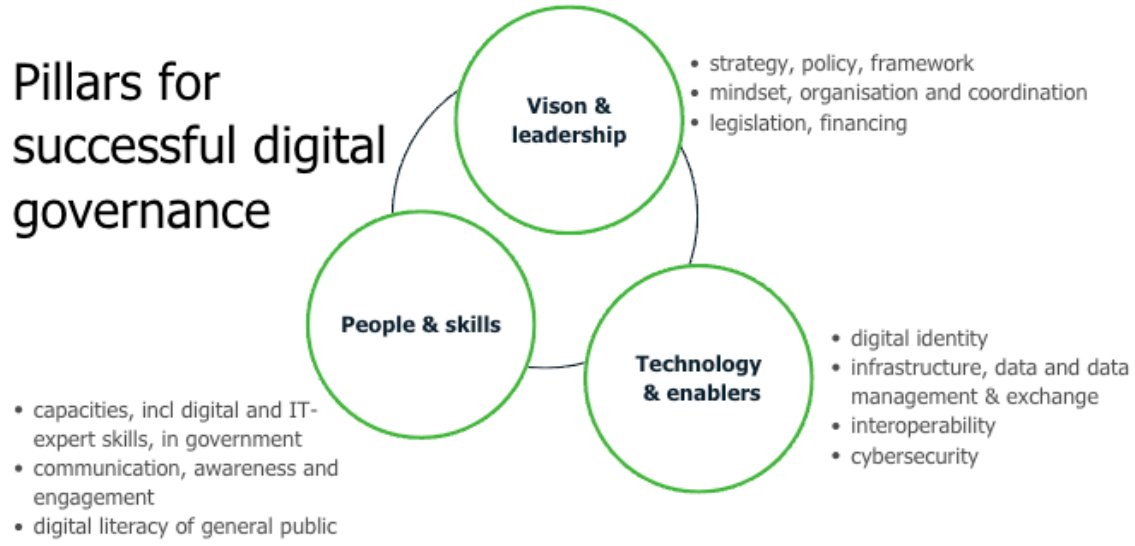


Figure 35 Key areas for successful digital governance.

Capacity-building is a process – it is never finished, never completed and there will always be room for further progress. Driving digital transformation with a structured capacity-building approach ensures that knowledge is retained at the institutional level rather than just at the individual level and retains capacity despite the turnover of government and public officials.

The central aim of capacity-building is to increase competence (mindset, knowledge, skills).

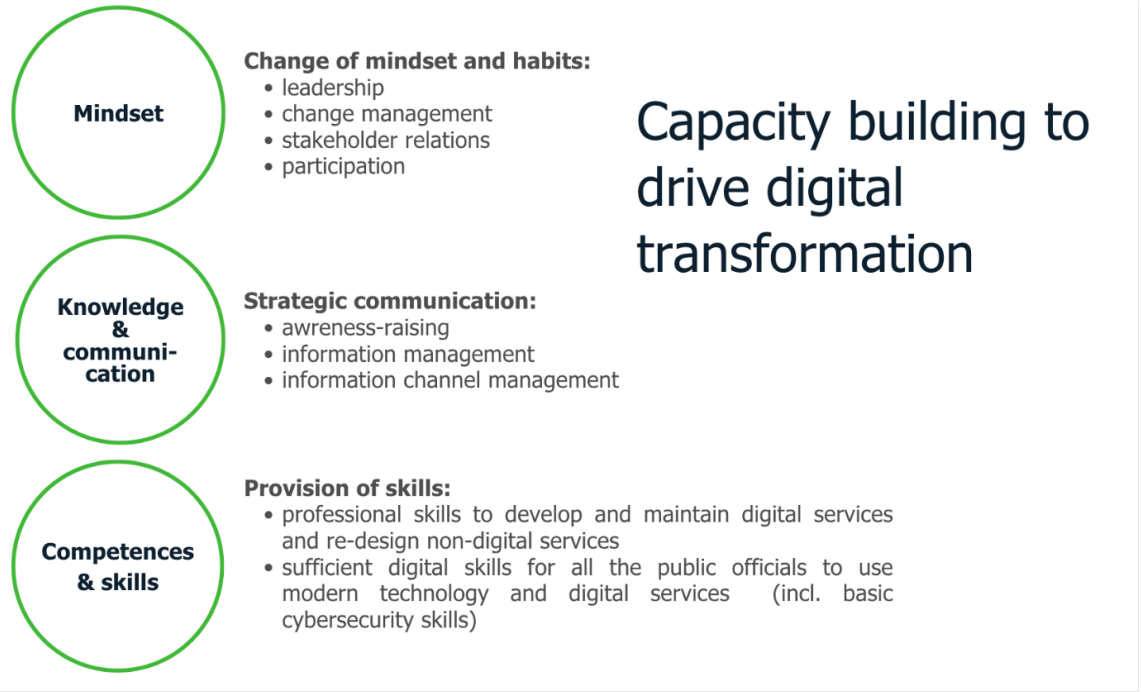


Figure 36 Capacity building to drive digital transformation.

In addressing building digital skills and competencies for digital transformation goals, the actions must be designed to promote a sustainable solution and focus on supporting the aim of digitally empowering the public sector and citizens while being guided by the digital transformation strategy and roadmap. The government, private sector, and civil society organisations can play a critical role in addressing the digital divide by working together to identify and implement solutions. By narrowing the digital gap, the government can promote greater equality, prosperity, and social inclusion for its citizens.

To implement strategic goals institutions, there is a need for internal experts (including IT) and implementation teams with advanced skills to execute the government's digital vision and strategy, for example, to implement business process reengineering, design citizen-centric services, ensure data quality and cybersecurity throughout the services, to maintain IT architecture and user support, and manage IT projects.

6.2 Capacity Building Framework

Digital transformation requires significant changes in institutions' operations, including adopting new technologies, processes, and business models. High-level and mid-level management in government institutions are vital Change Agents, helping to manage the transition, address resistance and change fatigue, and ensure that employees are engaged and supportive of the transformation efforts. Their leadership is essential in communicating change benefits, building consensus, and motivating their teams.

The framework provides a structured path forward and encompasses the development of learning, development and training programs that address mindset, knowledge, and

skills, ensuring that all stakeholders and Change Agents are prepared for the digital transformation journey. A structured approach ensures a capacity-building framework that aligns with the digital transformation objectives.

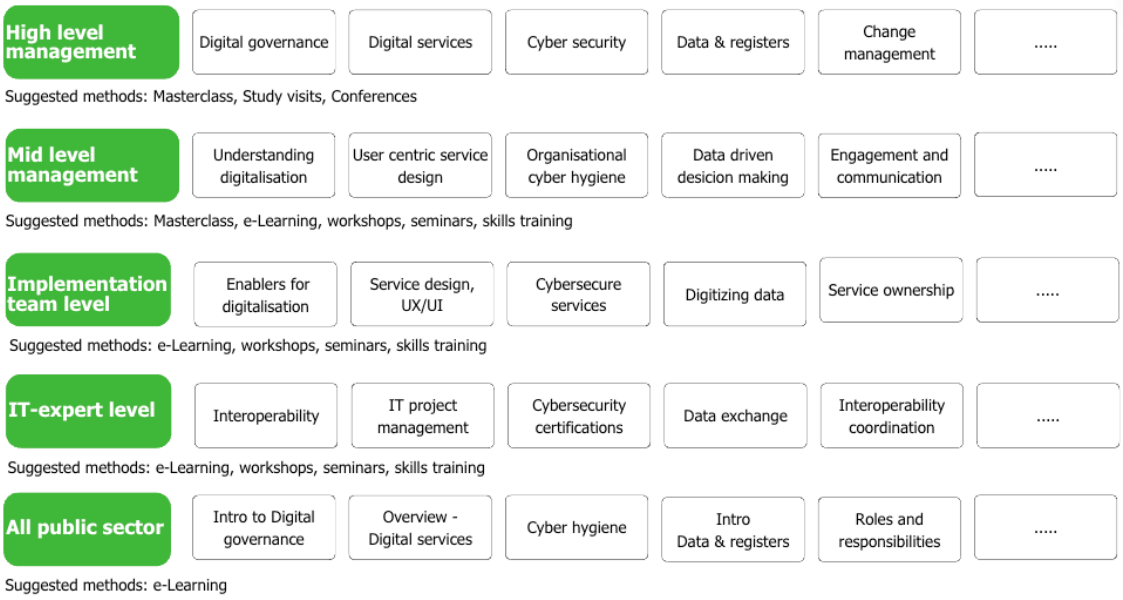


Figure 37 Training topics and methods mapping

High-level management needs to understand the **main digitalisation topics** and is focused on developing the mindset and awareness of the possibilities, benefits, and opportunities of digital transformation, as well as managing the overall process.

Mid-level management needs to be aware of how to implement digital transformation initiatives effectively.

Implementation teams and IT experts require the mindset, awareness, and technical skills necessary to execute digitalization projects. The Change Management workshop highlighted the following **technical skills:**

- Software Development: Programming languages (Java, Python, C++), scripting (SQL, Bash), frameworks (Spring, Django)
- project management,
- networking,
- system administration,
- data analysis,
- Machine learning/AI,
- cloud computing,
- cybersecurity.

The Change Management workshop highlighted the importance of soft skills, such as communication, teamwork, and change management, for capacity building. So, in

addition to digital transformation-related topics, there is a need for **power (soft) skills** to address the changes effectively and efficiently:

- leadership and management skills,
- communication skills,
- teamwork,
- problem-solving and critical thinking,
- time management and organization,
- strategic thinking,
- work ethic and initiative,
- customer service (if relevant),
- interpersonal skills,
- learning agility,
- information processing,
- negotiation (if relevant),
- integrity,
- self-awareness,
- self-management,
- situational awareness.

The workshop also discussed the importance of digital transformation-related capacity building and skills and the need for better communication of current capacity building and upskilling activities.

The entire public sector workforce should be aware of digital transformation concepts, service design, data management, and cybersecurity, and possess basic digital skills. This structured approach ensures that all levels within the public sector are prepared and equipped to contribute to the digital transformation journey.

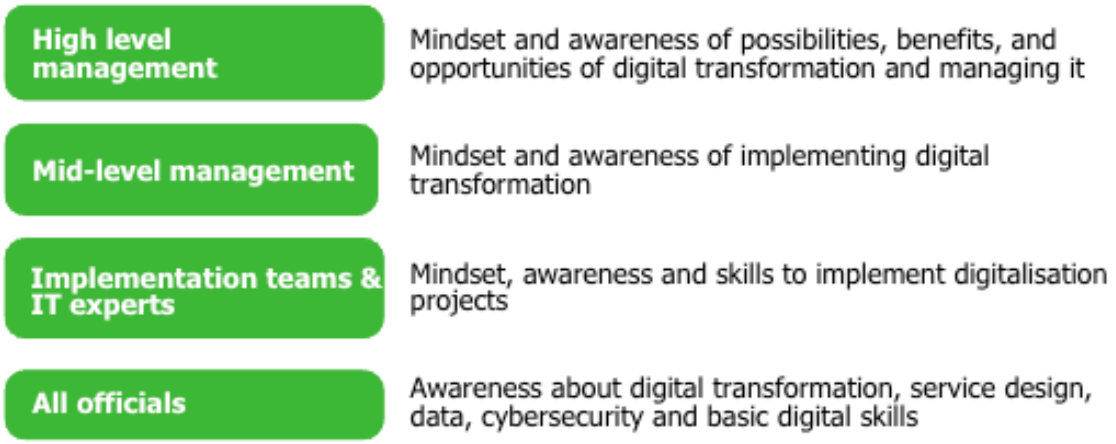


Figure 38 Capacity building target groups

For the digitalisation goals, it emphasized the **need for a centralised and standardised capacity-building framework** and curriculums. A centralised framework ensures that all training programs follow certain standards and quality measures, thus enhancing the learning experience. It is easier to expand training programs to reach a wider audience and ensure accessibility for all participants, regardless of location or background. A planned approach leads to cost savings and a more efficient allocation of resources and enables consistent measurement and evaluation of training program effectiveness, providing valuable data for continuous quality improvement. Moreover, a centralised framework fosters collaboration and knowledge sharing among stakeholders.

When designing capacity-building frameworks and learning programmes, **the architecture vision and central components must be taken as a starting point.**

The first step in the process will be identifying learning gaps and pinpointing areas where learners lack knowledge, motivation, habits, information, or skills necessary for success. Different gaps need a different approach when designing learning activities.

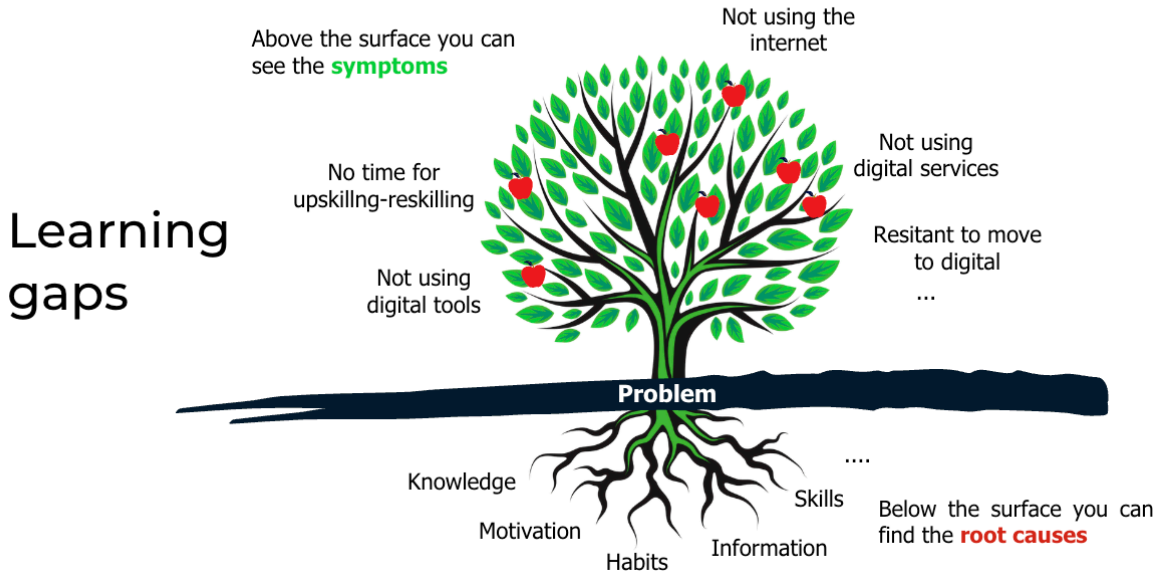


Figure 39 Learning gaps and problem tree

For the next steps:

- **Design more specific training plans and programs:** This involves outlining the specific goals and objectives of the training, as well as the content that will be covered.
- **Describe learning outcomes:** This means identifying what learners should be able to do by the end of the training. Learning outcomes (for example Bloom's

Taxonomy[3]) should always be specific and measurable. The number of learning outcomes per training depends on the length and level of the training. Usually,

Figure 40 SMART outcomes

there are up to five learning outcomes for a one-day training. Good learning outcomes could follow the SMART rule.

- **Identify learning gaps:** This includes assessing the knowledge, motivation, habits, information, or skills that learners currently have, and identifying any areas where they need improvement.
- **Decide on the methods.** When designing e-learning engage the instructional designer and focus on the learning outcomes agreed upon beforehand rather than overwhelming learners with all the information possible about the topic. This enables them to create relevant learning activities, engaging and appealing to the learner. Also, a learning designer's understanding of their target audience is essential, to know their retention ability and what visual mix motivates them to learn. The design and creation of an e-course must consider the challenges of modern adult learners and future learning, including:

  a) E-course is created using modern instructional design theory.
  b) Completion of one e-course or module takes the learner approx. 25-45 minutes and can consist of short up to 10-minute lessons that form a whole (for example, micro-learning as part of macro-learning).
  c) The e-course includes self-checking and evaluation activities that provide automatic feedback across all learning outcomes, interactive activities, and/or visual materials (videos, animation, graphics) to keep the learner motivated, practice skills, reflect, etc. and references to more in-depth material or the course (s). tests with feedback.
  d) The e-learning environment and the e-courses should be created with Web Content Accessibility Guidelines (WCAG) in mind and should be available at any time from any device.

[3] https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

e) Learning management systems (LMS) and e-course content should be accessible without paid software, compatible with common operating systems, reasonable data volume and so on.

- **Design curriculums:** This involves creating a structured learning plan that outlines the content, activities, and assessments that will be used to achieve the training objectives.
- **Deliver training:** This refers to the actual process of providing the training to learners. This can be done in a variety of ways, such as in-person instruction, online learning, or blended learning.
- **Monitor and adjust:** This involves evaluating the effectiveness of the training and adjusting as needed. This may include collecting feedback from learners, assessing their learning outcomes, and making changes to the training content or delivery methods.

When to develop e-Learning courses in-house:

- Unique content: If the content is specific to the organisation or geographic area and is unlikely to be commercially available, developing the courses in-house may be more beneficial.
- Language proficiency: If target learners are not fluent in the languages where pre-existing content is available, developing courses in-house can ensure that the content is tailored to their language needs.
- Customisation: If an elevated level of customisation and full control over content is required, developing courses in-house allows you to create content that aligns precisely with your program's objectives and requirements.
- Subject matter expertise: If subject matter experts are within the organisation who can contribute to developing the courses, developing the content in-house may be more efficient and cost-effective.
- Long-term maintenance: If there is capacity and resources to maintain and update the content on an ongoing basis, developing courses in-house gives you complete control over the content's maintenance and updates.

When to use existing courses available from different service providers/environments:

- Standardised content: If the content deals with a standard body of knowledge or widely used skills for an industry or target population, using existing courses already available from reputable service providers may be more practical.
- Rapidly shifting skilling needs: If the skilling needs of learners are constantly evolving, using existing courses allows you to access fresh content that the service providers regularly update.

- Language proficiency: If learners are proficient in the languages where pre-existing content is available, existing courses can provide a wide range of options without translating or customising.
- Diverse target learners: If a diverse set of learners with varied skill development needs are present, using existing courses allows you to offer a broader range of options and cater to different learning preferences.
- Cost and time considerations: If budget and time constraints exist, using existing courses can be more cost-effective and time-efficient than developing in-house courses.

7 Recommendations

The outcomes of the workshops carried out in the first half of the year in Harare, Chinhoyi, and Mutare, all highlighted the need for change, both technological and the way government work is conducted.

Recommendation 1 – Defining and forming a governance structure

Defining and forming a governance structure can be seen as a starting point before embarking on the digital transformation journey. The governance structure must be discussed and agreed upon within the government structures and enshrined into a legal decision or document. Open discussion of how things will be governed gives the governing body moral authority to carry out duties, while the legal decision gives the body formal rights to do so.

1.1 eGA suggests forming the governing body under the e-Government Technology Unit of the OPC and nominating representatives at least from the following institutions:

1. Ministry of Information Communication Technology, Postal and Courier Services
2. Public Service Commission
3. Ministry of Finance

The e-Government Technology Unit of the OPC would be responsible for leading the work of the governing body and coordination with other MDAs.

Ministry of Information Communication Technology, Postal and Courier Services would oversee the architectural components of the digital transformation.

The Public Service Commission would be assigned to organise civil servant's capacity building and skills uptake.

The Ministry of Finance is key in providing sufficient funding for the smooth digital transformation journey.

1.2 eGA encourages engaging all stakeholders in the change process.

Designated representatives from MDAs could form an agile advisory body – a formal or a loose network of change agents carrying out the agreed activities within their respective MDAs essential to the digital transformation journey.

1.3 eGA strongly recommends continuing with co-creational and collaborative activities to use the full potential of the MDAs, overcome the resistance to change, break down silo-mentality, and address the change fatigue.

Recommendation 2 – Creating a capacity-building framework

Creating a centralised and standardised capacity-building framework and curriculums related to digitalisation and establishing the Enterprise Architecture are needed to ensure consistent quality and accessibility in training programs. This approach allows for wider reach, cost savings, efficient resource allocation, and better measurement of program effectiveness. Additionally, it promotes collaboration and knowledge sharing among stakeholders. The activity should be considered as a joint venture between OPC, the Public Service Commission and other relevant stakeholders.

Recommendation 3 – Communicating change initiatives

PR and communication professionals should be embedded in the change process for a successful digitalisation process. Their role should extend beyond just messaging; they need a seat at the strategic table to ensure a unified narrative. Craft compelling stories that resonate with Zimbabwe's unique identity. Most importantly, open, and two-way communication with all stakeholders should be prioritised. Foster a sense of shared ownership with the message "We are the change that will directly benefit our citizens," so everyone feels invested in making the digital leap a success.

In summary, the emphasis for the successful implementation of whole-of-government architecture should be on:

- Establishing a coalition of change agents to support the change process.
- Establishing a sense of urgency for capacity-building (in the field of digitalisation).
- Establishing communication guidelines for all MDAs to communicate change.
- Establishing a culture of engagement within the change process.
- Establish good governance in the field of ICT with clear roles and responsibilities.

8 Abbreviations

ABB	Architecture Building Blocks
G2B	Government to Business
IPS	Integrated Public Service
IS	Information System
MDA	Ministries, Departments and Agencies
OPC	Office of the President and Cabinet
ToT	Training of Trainers
ZWoGA	Zimbabwean Whole of Government Architecture
WCAG	Web Content Accessibility Guidelines

9 Annexes

9.1 Change Management Communication Plan

Table 32 Change Management Communication Plan Template

EVENT / ACTION / STRATEGY	PROJECT PHASE(S)	EST. DATE OF EFFECT	TARGETED STAKE-HOLDERS	IMPACT LEVEL	REASON	METHOD
Announcement of Change						
Change Implementation Training						
Activity 3						
Activity 4						
Explanations:						
TARGETED STAKEHOLDERS: List both internal and external stakeholders if needed.						
IMPACT LEVEL: Highly Impacted: This group directly experiences the biggest changes due to the policy. They might need more in-depth information and support during the transition. Moderately Impacted: This group experiences some impact but might require less detailed information. Low Impact: This group experiences minimal changes but should still be informed.						
REASONS TO COMMUNICATE: Examples: To make sure everyone is aware of the change. To explain the reasons for the change. To get people on board with the change. To minimize disruption caused by the change. To address any concerns people may have about the change. To provide information on how the change will be implemented**.**						
METHOD OF COMMUNICATION:						

Examples: Printed materials (brochures, flyers, physical mail), public notices (formal announcements), press conferences, events, websites/intranet, email, texting, white papers, handbooks, meetings with relevant officials, intranet, demos, meetings, workshops, training.

9.2 Sample Timeline for Communication Activities

Twelve weeks prior to introducing Enterprise Architecture:

- Additional research, including the status of the change initiative, what target groups are needed etc.

Ten weeks before introducing Enterprise Architecture:

- defining goals and objectives of the communication program,
- defining the key audiences,
- detail the communication strategies.

Eight weeks prior to introducing Enterprise Architecture:

- develop key messages,
- begin developing communication materials,
- begin outreach to higher-level stakeholders.

Six weeks prior to introducing Enterprise Architecture:

- Develop press kit and media lists.

Four weeks prior to introducing Enterprise Architecture:

- one-on-one meetings (roadshows) with key influencers,
- shoot video materials if needed,
- media training to spokespersons if needed.

Two weeks prior to introducing Enterprise Architecture:

- create a press release announcing the Enterprise Architecture,
- draft and distribute a press release,
- publish any other supporting materials,
- start hosting forums/workshops.

As the introduction of Enterprise Architecture begins:

- draft articles,
- arrange interviews,
- distribute newsletters etc.

After the introduction:

- seminars, workshops with feedback gathering,
- analysing feedback and correcting messages and actions if needed.

9.3 Key Feedback

Key feedback from the workshops that have been the basis for recommendations covered in this report in more depth:

- Defining roles and responsibilities.
- Co-creational defining of change – gaining mutual trust among MDAs.
- Thinking as a team of change agents and creating synergies.
- Utilising the thematic working groups better, communicating in the current organisational structures and re-organising communication with changes in the structure.
- Aligning our actions and cascading them to the stakeholders and ensuring buy-in from stakeholders.
- Using incentives and praise/attention for those who help to push change.
- Implement a new working culture.
- Address concerns and fears.
- Skills, skills, skills.
- Creating and following communication principles across MDAs.
- Use clear metaphors.
- Engaging communication teams early in the process – they can also be the change agents or early adopters.
- Communicate success stories early and continue throughout the process.
- Celebrate small wins.

9.4 Sample Internal Workshop for Change Agents

Leading the Enterprise Architecture Change Initiative

Target Audience: Change Agents across the MDAs.

Time: 3 Hours

Workshop Objectives:

- Equip change agents with strategies to navigate common change barriers.
- Identify and leverage change enablers for successful implementation.
- Develop practical communication activities for change initiatives.
- Explore tools and techniques for capacity-building and engagement.
- Enhance cooperation between MDAs.

Agenda

Welcome & Introductions (15 minutes):

- Icebreaker activity to build rapport and introduce participants.
- Workshop overview and objectives.

Understanding Change Management (30 minutes):

- Interactive presentation on the change curve and common psychological responses to Change.
- Group discussion: Based on the feedback from the initial workshops, identify potential barriers and enablers for the upcoming change initiative.
- Introducing the vision for Enterprise Architecture and changing the timeline (if available)

Break (10 minutes):

- Networking opportunities and refreshments.

Communicating Change Effectively (45 minutes):

- Interactive activity: Develop key talking points for the upcoming change initiative.
- Discussion: Strategies for addressing resistance and promoting buy-in.

Building Capacity & Driving Engagement (45 minutes):

- Interactive presentation on tools and techniques for capacity-building, including training, coaching, and mentoring.
- Sharing best practices for ongoing communication and feedback collection.

Wrap-Up & Action Planning (20 minutes):

- Q&A session for any outstanding questions.
- Development of individual action plans for participants to implement key takeaways.
- Closing remarks and next steps.

Materials:

- Presentation slides on change management principles and communication strategies.
- Flipcharts and markers for group activities.
- Handouts with key takeaways and resources for further learning.

9.5 Sample Press Release for Communicating Change

Zimbabwe Government Embarks on Digital Transformation Journey with Enterprise Architecture

The Government of Zimbabwe announced a significant step towards a more integrated and efficient digital future by developing a whole-of-government Enterprise Architecture (EA). This initiative will create a comprehensive blueprint for IT systems and infrastructure, ensuring seamless delivery of digital services to citizens and businesses.

"Our vision is to leverage technology to empower our people and fuel economic growth," said [Name and Title of Government Official]. "A robust Enterprise Architecture is the foundation for achieving this vision. It will allow us to optimise IT investments, improve service delivery, and enhance collaboration across government agencies."

The new EA will encompass various domains, including:

- Integrated Public Service Architecture: Assisting public service owners in (re)-designing their public services to benefit digitalisation and provide better public services for citizens.
- Application Architecture: Providing a set of common functionalities as techno-organisation platforms that ease the burden of creating interoperable information systems in each MDA.
- Data Architecture: Establishing clear guidelines for data management and sharing across agencies.
- Technology Architecture: Ensuring adequate infrastructure, communication, and other baseline IT services to be operational from the MDAs on demand.
- Security architecture - Suggesting a standardised approach for implementing security measures and emergency response capabilities to keep MDAs and their information systems security aware.

The development of the EA will involve collaboration between government ministries, departments, and private sector partners. The government is committed to building capacity through training programs and certifications for IT professionals specialising in Enterprise Architecture.

"This is a transformative initiative that will require a collaborative effort," said *[Name and Title of IT Official]*. "We are confident that by working together, we can create an EA that delivers tangible benefits for all Zimbabweans."

Benefits of the Enterprise Architecture:

- Improved citizen and business experience through integrated service delivery.
- Increased efficiency and cost savings through optimised IT investments.

- Enhanced data governance and security.
- Increased agility and responsiveness to changing needs.

Next Steps:

The government will soon announce the formation of a dedicated Enterprise Architecture team and launch a public consultation process to gather stakeholder feedback.

[Government website/social media] will provide ongoing updates on the development of the Enterprise Architecture.

Contact:

[Name and Title of Spokesperson] [Email Address]

9.6 Sample Social Media Posts

9.6.1 Platform: Facebook

Headline: Building a Better Together: Zimbabwe's Whole-of-Government Enterprise Architecture

Body: We are the change that will directly benefit our citizens! The Government of Zimbabwe is developing a new Enterprise Architecture (EA) to streamline operations, making it easier for you to interact with government agencies.

This EA, inspired by the enduring resilience of the Balancing Rocks, will:

Foster collaboration across ministries, symbolising our unity and diversity.

Standardise IT systems for greater efficiency.

Improve access to government services online, like uncovering riches from the Great Dyke, for all Zimbabweans.

Despite speaking many languages, we speak the same language in terms of creating a better life. Stay tuned for updates on how this EA, like a Baobab tree, will grow our government services into a well-functioning ecosystem!

#ZimDigital #eGovernmentZimbabwe

9.6.2 Platform: LinkedIn

Headline: Zimbabwe Embarks on Transformational Journey with Whole-of-Government Enterprise Architecture: We Are the People to Make the Change Impactful

Body: The Government of Zimbabwe is proud to announce the development of a comprehensive Enterprise Architecture (EA), a **uniquely Zimbabwean approach** to digital public services.

This initiative, inspired by the enduring strength of the Balancing Rocks, will:

- Foster better collaboration between government agencies, symbolising our national unity.
- Enable the delivery of improved citizen services, directly benefiting our people.
- Support the government's digital transformation goals, creating an ecosystem like a flourishing Baobab tree.

This project represents a significant step forward. We invite IT professionals, government officials, and interested citizens to follow our progress and contribute to this national endeavour.

#GovernmentIT #eGovernmentZimbabwe #DigitalTransformation

9.6.3 Platform: X

Post: Calling all Zimbabweans! #WeAreTheChange to build an impactful #GovernmentEA for a uniquely Zimbabwean approach to service delivery! #ZimDigital #eGovernment Stay tuned for updates on this exciting transformation!

9.7 Basic Digital Competencies for All Public Sector

The value of adapting already existing and more widely spread and used frameworks in addition to efficient use of resources, are also the benefits coming from already designed and publicly available training programmes fit for the frameworks and assessment tools and tests. The latter is to measure the progress towards the targets set as well as the efficiency of the programmes/measures implemented.

For example, those frameworks can be considered as inspiration for further digital skills training programmes:

- "National standards for essential digital skills" by the Department of Education of the UK Government (updated in 2019).
- "The Digital Competence Framework" (DigComp) is widely used as a base for many national digital competency frameworks. The Digital Competence Framework for Citizen (DigComp) provides a common understanding of what digital competence is. The present publication has two main parts: the integrated DigComp 2.2 framework provides more than 250 new examples of knowledge, skills and attitudes that help citizens engage confidently, critically, and safely with digital technologies, and new and emerging ones such as systems driven by artificial intelligence (AI).
- Online tests based on the DigComp framework are also available for free – for example, Europass Test/Digital Skills and Jobs Platform, IT fitness, DigComp. ·
- "A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2" by UNESCO, Appendix 1 lists more digital literacy frameworks.

9.8 Learning Programme for Top-level Executives

Objective

Digital transformation in government means more than just moving services online. Instead, it is a mindset change in the way the public sector operates, including the digital transformation of internal processes, and the changes in culture and ways of working that technology can encourage.

This capacity-building programme aims to give top-level executives from different institutions knowledge on how to initiate digital transformation in government and change how organisations work.

The programme supports networking amongst participants from different institutions to improve communication and supports the long-term goal to break down the silos and allows sharing of good experiences and lessons learned in that journey.

Target group

Key roles from different governmental authorities, ministries/agencies, and institutions.

Programme outline

The programme should include at least 5 face-to-face seminars (1-2 days each) from top-level lectures/senior experts in the field as well as workshops to discuss the topics amongst the participants. The programme should run for a minimum of 6 months so participants have enough time to initiate and run digital transformation processes in their ministry/agency and put the learning experience into practice while taking part in the course. Between the seminars, top-level mentoring/coaching of the participants is recommended.

Topics to be covered:

- possibilities, benefits, and opportunities of digital transformation,
- technological trends, cloud, data, and AI,
- cybersecurity,
- digital transformation of processes, user-friendly and customer-centric services,
- managing digital transformation (for example leadership and change management, agile management, agile working solutions),
- communicating digital transformation (how to get different stakeholders on board, main communication messages and channels).

Outcome

During the training program, participants will draft their own ministry's/agency's digital readiness review and define digital transformation goals and a long-term digital transformation roadmap.

9.9 Learning Programme for Mid-Level Management

Objective

This capacity-building programme aims to give mid-level executives knowledge and skillsets on initiating and implementing digital transformation in public office and changing how organisations and departments work.

The programme supports networking amongst participants from different institutions to improve communication and supports the long-term goal to break down the silos and allows sharing of good experiences and lessons learned in that journey.

Target group

Mid-level managers, team leaders and personnel responsible for digital transformation in different ministries/agencies, and institutions.

Programme outline

The programme should include at least 5 face-to-face seminars (1-2 days each) for lectures and workshops to discuss the topics and practical skills training run for a minimum of 6 months. Between the seminars, mentoring and coaching the participants are recommended.

Key elements of the programme and curricula should be designed centrally, and it is recommended to have centralised training of trainers. Training programs for target groups should be available to all public officials interested and accessible all over the country. In collaboration with universities, it could be possible to use their premises.

Topics to be covered:

- overview of possibilities, benefits, and opportunities of digital transformation,
- overview of technological trends, cloud, data, and AI,
- service design principles – the digital transformation of processes and services (including internal processes), user-friendly and customer-centric services,
- data management, data analysis and using data for decision-making,
- technological platforms and interoperability frameworks,
- cybersecurity in processes and e-services, and cybersecurity for public officials,
- agile methods of work - in management and work processes,
- managing digital transformation and power skills (this ranges from listening and communicating, to leading teams, empathy, teamwork, leadership and change management),
- main principles of effective communication and awareness raining to support digital transformation.

Outcome

During the programme, participants will develop their own ministry's/agency's short-term digital transformation roadmap based on their digital transformation goals.

9.10 Learning Programme for Public Service Design and Reengineering

Objective

This capacity-building programme aims to give knowledge, skillset, and hands-on experience on how to design or redesign public services.

The programme supports networking amongst participants from different institutions and supports the long-term goal to break down the silos and allows sharing of good experiences and lessons learned in that journey.

Target group

Service managers, service owners, and product owners, service design teams. No previous experience is needed.

Programme outline

The programme should include 4-5 face-to-face seminars (each 1-2 days) for theoretical overview and practical workshops for a minimum of 6 months. Between the seminars mentoring and coaching the participants is recommended.

Key elements of the programme and curricula should be designed centrally, and it is recommended to have centralised trainer training programmes. Training programmes for target groups should be accessible all over the country and available to all interested.

Topics to be covered:

- Introduction to digital service development. A theoretical introduction to user-centric service development principles, key focus points and steps – how to identify a problem and engage stakeholders.
- Practical workshop: digital service development – service management - role and responsibilities of the service owner, management of the service, indicators, financing.
- Practical workshop: digital service development – planning. Practical workshop on how to start e-service development - the creation of a service development team, defining a problem to be solved with the service, data-based solutions, service roadmap, identification of existing solutions, limitations, and requirements (including legal and technological), stakeholder engagement.
- Practical workshop: digital service development, data, and interoperability. How data is created, data life cycle, how to use data and present data, and possibilities in the future - machine learning and AI.

- Practical workshop: digital service development – security requirements. Identification of possible security risks, the definition of requirements, and design of secure services.

Outcome

During the program, participants develop a service roadmap and short-term development plans for their own (digital) service.

9.11 Sample Learning Programme for Data-Driven Decision-Making for Mid-Level Management

Objective

This capacity-building programme aims to give mid-level executives an understanding of how to use data to guide strategic business decisions and what tools to use for communication.

The programme supports networking amongst participants from different institutions to improve communication and supports the long-term goal to break down the silos and allows sharing of good experiences and lessons learned in that journey.

Target group

Mid-level managers, team leaders and personnel responsible for digital transformation in different ministries/agencies, and institutions.

Programme outline

The programme should include 2 days of face-to-face seminars for theoretical overview and practical workshops.

Key elements of the programme and curricula should be designed centrally, and it is recommended to have centralised trainer training. Training for target groups should be accessible all over the country and available to all interested.

Topics to be covered

- overview of data-driven decision-making. A theoretical introduction to data-driven decision-making and the decision-making process. Examples of dashboards and good usage of data in governments.
- Overview of data management. Categories of data, processes, sources, data quality, collection and data governance and roles needed.
- Practical workshop: Identify the problem and define data to understand and solve it. Find data, including missing data, and evaluate data quality. Formulate the solution.
- Practical workshop: data visualisation. A theoretical introduction to different data visualisation tools and practical data visualisation exercises.

- Practical workshop: communicating the result. Planning the communication and preparing messages to stakeholders.

Outcome

During the program, participants will use their institution's data to offer a solution to the identified problem using data visualisation techniques that bring numbers to life.

10 Bibliography

Cole, R., King, D., & Sowden, R. (2015). Defining change. In R. Smith, D. King, R. Sidhu, & D. Skesley, *The Effective Change Manager's Handbook. Essential guidance to the change management body of knowledge* (p. 111). Kogan Page Ltd.

Government of Zimbabwe. (2024). *Policy for ICT.*

Government of Zimbabwe. (2022). *The Zimbabwe National Vision 2030.*

Kotter, J. P. (2012). *Leading Change.* Boston: Harvard Business Review Press.

Smith, R. (2015). A change management perspective. In D. K. Richard Smith, *Teh Effective Change Manager's Handbook. Essential guidance to the change management body of knowledge* (pp. 1-77). Kogan Page Limited.

Delivering a seamless Government experience

D5-3 Roadmap

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

1 Introduction

This document, developed by the e-Governance Academy in collaboration with the Government of Zimbabwe within the " An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" project, represents a synthesis of insights and ideas gathered through workshops, online meetings, and on-site engagements with stakeholders. Leveraging best practices and drawing upon the expertise of the e-Governance Academy's team, the Zimbabwean vision for enterprise architecture has been tailored to meet specific needs and objectives.

Please note that this document is a snapshot of the project's findings and status at the time of its creation. It is subject to ongoing refinement and revision as the project evolves and new information becomes available. The Government of Zimbabwe, under the guidance of the Office of the President and Cabinet, will oversee future updates and iterations.

This document serves as a resource for planning and implementing initiatives related to enterprise architecture development within the Government of Zimbabwe. By providing a comprehensive framework and guiding principles, it aims to contribute to the successful realization of the country's digital transformation goals.

While architecture deliverables for the Zimbabwean Whole of Government Architecture are descriptions of statical future situations the change management deliverables provide methods and tools for reaching the desired target state. The current deliverable - roadmap - is a concentration of recommended activities oriented primarily for the team responsible for the governance architecture but also the core lead of other architecture domains.

The roadmap should be seen as an initial document for planning activities and should be regularly revised and updated to reflect on the real-life situation. The changes that will impact the roadmap can be either the completion or lagging of some of the tasks or even a shift in the target state.

The roadmap is presented as a table where each activity is presented in the order of execution.

2 Roadmap

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
CM1	Form a Governance structure	Change Management	Governing body formed, roles and responsibilities defined, clear understanding and acceptance across MDAs, enshrined into legal document	OPC in co-operation with MDAs	Defining and forming a Governance structure is a starting point before embarking on the digital transformation journey. The Governance structure must be discussed and agreed upon within the Government structures and enshrined into a legal decision or document. Open discussion on how things will be governed gives the governing body moral authority to carry out duties, while the legal decision gives the body formal rights to do so. See also SA1, SA2 and SA7 about governing body of Security Architecture.	3 months	
CM2	Establish a Coalition of Change Agents to support the change process	Change Management	Designated representatives from MDAs engaged in change process	Newly formed governing body	Designated representatives from MDAs could form an agile advisory body – a formal or a loose network of change agents carrying out the agreed activities within their respective MDAs	3 months; engagement continuous throughout	CM1, together with AV1

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
					essential to the digital transformation journey. eGA strongly recommends continuing with co-creational and collaborative activities to use the full potential of the MDAs, overcome the resistance to change, break down silo-mentality, and address the change fatigue.		
CM3	Create a Capacity-Building Programme	Change Management	Learning, capacity building and skills uptake programme for civil servants	Newly formed governing body or designated MDA (Public Service Commission)	Civil Servants in different formal structures and levels must be equipped with necessary knowledge and skills to carry out and aid digital transformation in their respective fields.	Analysis of existing capacity– 3 months Defining TO-BE – 3 months Creating a programme – 3-6 months	AV2, CM2
CM4	Formulate Communication Guidelines	Change Management	MDAs communicating the change in a co-ordinated manner	Newly formed governing body or a special	Communication plays a key role in disseminating the urgency for change and stakeholder buy-in	3 months; execution continuous throughout	AV3

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
				communication person/team/unit			
AV1	Assign an owner for each Architecture domain and Foundational Building Block (Foundational Projects)	Architecture Vision & Governance Architecture	Each architecture domain has a clearly identified position and person who will be the owner the activities of its specific domain.	OPC eGov unit	Each domain and key building block must be assigned an owner. See also SA1, SA2 and SA7 about governing body of Security Architecture.	1 month	CM1
AV2	Phrase the domain and Building Block (Foundational Project) Service Statement	Architecture Vision, Governance Architecture	Statement of what the domain / building block delivers for its users.	Each domain owner	Requires the owners to go through ZWoGA, discuss with its stakeholders/users and with other domain/building block owners to define their work essence. ZWoGA provides functional generic description - user oriented "Service Offering" must be defined by the owners. The service statements must not be overlapping and be motivated from architecture goal/vision.	1 month	AV1

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
AV3	Clarify and measure the baseline of KPI	Architecture vision, Governance Architecture	Established baseline for monitoring the progress in the future.	Governance Architecture owner	Architecture Vision provides input for KPIs, these must be refined to practical metrics and the measuring procedure described so that in the future the measuring can be repeated.	1 month	AV1
AV4	Establish Policies Working Group	Architecture Vision, Governance Architecture	A semi-formal working group from architecture domains and key stakeholders is composed to overview policy drafting process.	Governance Architecture owner	While ad-hoc groups should be created to draft the process the overview of the process, prioritization of what to work with, and non-formal review of drafts requires a dedicated persistent semi-formal working group.	1 month for establishment of policies workgroup and initial ad-hoc policy drafting groups. Continuous operation for policy working group.	AV1
IA1	Assign Service Owners	IPS architecture	Persons responsible (service owners) are assigned and added to the Public Service Catalogue.	IPS architecture owner	Once public services are listed in the Public Service Catalogue, specific persons within the MDAs must be appointed as responsible for service	2 months	AV2

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
					lifecycle. Update of service owners list is a continuous process.		
IA2	Implement Service Design Framework and Task force (building block)	IPS Architecture	Public Service Design Framework is developed and accessible to the MDAs, and framework itself is tested within 6 pilot projects and adjusted, if needed.	IPS architecture owner	As described in requirements of Foundational Projects: methodology, toolbox and training materials together with e-learning platform. Start Taskforce work with pilot projects. Updating this Framework is a continuous process.	6 months for service design framework, 6 months for pilot projects.	AV2
IA3	Train Service Owners	IPS Architecture	Trainings for service owners are conducted.	IPS architecture owner	Cooperation with Public Service Commission	4 months	IA2
AA1	Establish Data Exchange Platform	Application Architecture		Data exchange owner		12 months	AV2
AA2	Establish Digital Identity Business Model	Application Architecture	Economical business model for digital identity defined.	Digital identity owner	As described in Foundational Project description.	18 months	AV2

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
AA3	Establish Digital Identity Solution	Application Architecture	Start of digital identity rollout	Digital identity owner	As prescribed by Digital Identity Business Model.	24 months	AA2
DA1	Compose and verify metadata model	Data Architecture	Initial meta-data model supporting ZWoGA	Data architecture owner (chief data officer)	Selection and refinement of different catalogues that are needed by stakeholders. Negotiation with other Architecture Domain and Building Block Owners.	3 months	AV2
DA2	Establish Data Catalogue	Data Architecture	Meta-data collection is initiated and listed in the Data Catalogue and can be accessed by the MDAs.	Data architecture owner	Solution selection, data collection process established in the catalogue by the service owners.	6 months	DA1
DA3	Develop/create Public Service Catalogue	Data Architecture	Public services are defined, described, a list of public services (service catalogue) is created and available to MDAs.	Data architecture owner	Solution selection (possible to combine with DA2) ed and information about currently provided services must be gathered from the MDAs. This task is related to the assignment of service owners. responses. To improve the data quality, information could be	2 months	DA1

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
					gathered during the interviews with MDAs.		
DA4	Develop and implement Metadata Quality Management Model	Data Architecture	Meta-data quality ensured as process.	Data architecture owner	Based on collected data develop and enforce quality constraints (timeliness, integrity, classifiably etc.). Quality measuring methodology creation and deployment.	9 months	DA2, DA3
SA1	Assign high-level Cybersecurity leadership	Security Architecture	Legal act or policy document, GCISO	OPC	Ideally, this should be assigned permanently through legislation or national strategy to a position or institution exercising the country's executive power with a governmental mandate, such as the Cabinet, a Government Minister, or a Ministry. Refer to Security Architecture chapter 4.1.	3 months	CM1, AV1
SA2	Form Cybersecurity Committee for security related	Security Architecture	A legal act endowing the Cybersecurity Committee, coordination body or format with the	GCISO	Include stakeholders from the public sector as well as selected representatives from private sector as well as from Civil Society. Cybersecurity Policy Coordination requires the presence of an official mechanism that	3 months	SA1

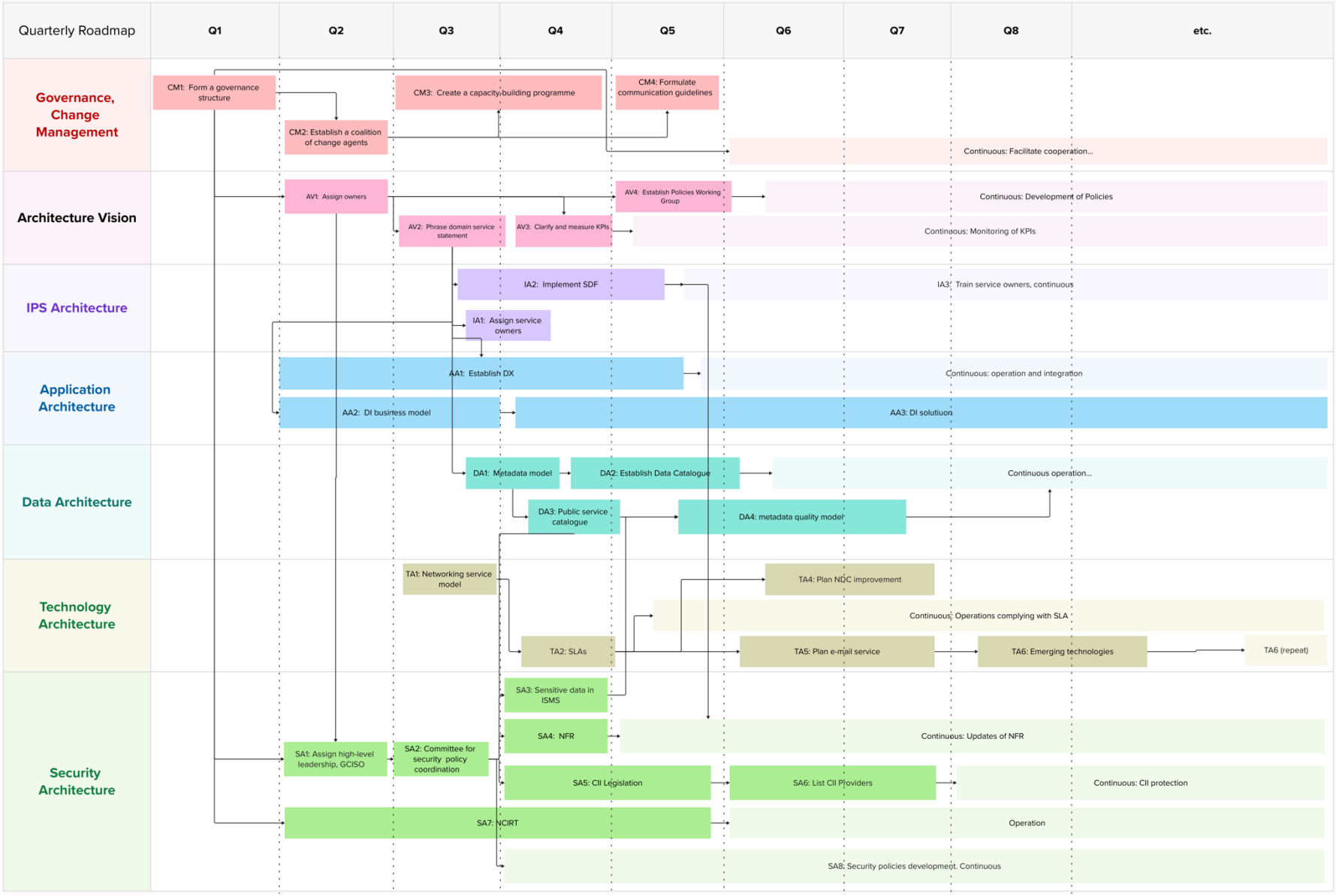
No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
	Policy Coordination		relevant responsibility		regularly engages relevant intra-Governmental, public, and private actors in Cybersecurity Policy Coordination and Cooperation. Such mechanisms may take various forms, such as permanent committees, councils, or working groups. Refer to Security Architecture chapter 4.2		
SA3	Define sensitive data Information System Management System (ISMS)	Security Architecture	ISMS Policy	Cybersecurity Committee	Framework of policies and procedures for systematically managing an organization's sensitive data. Refer to Security Architecture chapter 4.3	3 months	SA2, DA3
SA4	Publish Non-Functional Requirements (NFR)	Security Architecture	NFR	Cybersecurity Committee	The purpose of the requirements is to prevent the recurrence of problems. Refer to Security Architecture chapter 4.4	3 months. Continuous regular review and updates.	SA2
SA5	Enforce legal or administrative act about CII	Security Architecture	Legal or administrative act about CII	OPC according to the proposal from	Legislation that foresees a CII identification process, or the designation of such infrastructure by an	6 months	SA2

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
				Cybersecurity Committee	Administrative Act. Such designation has Cybersecurity implications for the infrastructure operator. Refer to security architecture chapter 4.5.		
SA6	Introduce list of Vital Service Providers	Security Architecture	Data in form of list, table, etc attached to the Legal Act (D4.6 4.5) about Vital Service Providers	OPC according to the proposal from Cybersecurity Committee	Refer to Security Architecture chapter 4.6.	6 months	SA5
SA7	Form Zimbabwe National Computer Incident Response Team (NCIRT)	Security Architecture	Organization of NCIRT	MICTPCS, working with POTRAZ	Please review ENISA publication "How to set up CSIRT and SOC". Refer to Security Architecture chapter 4.7.	12 months	CM1, AV1. Also TA1, TA2, TA4, AA1, AA3, IA2
SA8	Introduce additional Policies related with Cybersecurity	Security Architecture	Policies	OPC according to the proposals from Cybersecurity Committee and NCIRT	Set of policies should be decided in cooperation with Cybersecurity Committee and NCIRT to importance and urgency. Please refer possible set from Security Architecture paragraph 5.	18 months	SA2

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
TA1	Define Service Model for Networking	Technology Architecture	Operational model for Technology Architecture building blocks dividing organisational responsibilities.	OPC and Technology Architecture Owner	Division of services between Ministry of ICTPCS NDC and GISP must be cleared and how it is delivered to MDAs. Assign building block owner who will be responsible for respective building block service and its Roadmap.	3 months	AV2
TA2	Create Technology Services SLAs	Technology Architecture	Realistic SLA for current services (Networking and NDC)	Technology Architecture Owner	For networking, NDC and e-mail/calendar service. Refer to Technology Architecture Building Blocks.	2 months	AV2
TA3	Plan for Networking Building Block improvement	Technology Architecture	Improvement plan for adoption at highest level.	Networking building block owner.	Collect and analyse (potential) client requirements for 5-year perspective. Describe the gap, investment needs and operations cost for services as needed. Technology Architecture proposes structure of services while content must be negotiated with existing and potential clients.	6 months	TA1
TA4	Plan for NDC Building Block improvement	Technology Architecture	Improvement plan for adoption at highest level.	NDC Building Block Owner	Collect and analyse (potential) client requirements for 5-year perspective. Describe the gap, investment needs	6 months	TA2

No	Action	Domain	Result	Responsible	Comment	Duration	Prerequi-site
					and operations cost for services as needed. Technology architecture proposes structure of services while content must be negotiated with existing and potential clients.		
TA5	Plan for E-mail Service Building Block improvement	Technology Architecture	Improvement plan for adoption at highest level.	E-mail Building Block Owner	Collect and analyse (potential) client requirements for 5-year perspective. Include security requirements. Describe the gap, investment needs and operations cost for services as needed. Technology architecture proposes structure of services while content must be negotiated with existing and potential clients.	3 months	TA2
TA6	Analyse Emerging Technologies for potential	Technology Architecture	Input for the 2nd Architecture Development Cycle.	OPC and cooperation with Technology Architecture Owner.	While emerging technologies can be piloted their inclusion to the architecture should be a rational decision. The analysis should create a recommendation with potential operational and economical model for next architecture iteration.	4 months	TA1, TA2

A diagram presenting the overview across time is presented on the following page.


Quarterly Roadmap
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
etc.
Governance, Change Management
CM1: Form a governance structure
CM2: Establish a coalition of change agents
CM3: Create a capacity-building programme
CM4: Formulate communication guidelines
Continuous: Facilitate cooperation...
Architecture Vision
AV1: Assign owners
AV2: Phrase domain service statement
AV3: Clarify and measure KPIs
AV4: Establish Policies Working Group
Continuous: Development of Policies
Continuous: Monitoring of KPIs
IPS Architecture
IA1: Assign service owners
IA2: Implement SDF
IA3: Train service owners, continuous
Application Architecture
AA1: Establish DX
AA2: DI business model
AA3: DI solutiuon
Continuous: operation and integration
Data Architecture
DA1: Metadata model
DA2: Establish Data Catalogue
DA3: Public service catalogue
DA4: metadata quality model
Continuous operation...
Technology Architecture
TA1: Networking service model
TA2: SLAs
TA4: Plan NDC improvement
Continuous: Operations complying with SLA
TA5: Plan e-mail service
TA6: Emerging technologies
TA6 (repeat)
Security Architecture
SA1: Assign high-level leadership, GCISO
SA2: Committee for security policy coordination
SA3: Sensitive data in ISMS
SA4: NFR
SA5: CII Legislation
SA6: List CII Providers
SA7: NCIRT
SA8: Security policies development. Continuous
Continuous: Updates of NFR
Continuous: CII protection
Operation

Delivering a seamless Government experience

Compiled by the e-Governance Academy within the project "An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe" funded by the Government of Zimbabwe

Find out more:

D6-1

Requirements for Establishing Secure Data Exchange for the Government of Zimbabwe

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Abbreviations and Terms

Term	Definition
CA	Certification Authority
ICT	Information and Communication Technologies
MDAs	Ministries, Departments and Agencies, Zimbabwe
MICTPCS	Ministry of Information Communication Technology, Postal and Courier Services, Zimbabwe
OPC	Office of the President and Cabinet, Zimbabwe
PKI	Public Key Infrastructure
POTRAZ	Postal and Telecommunications Regulatory Authority, Zimbabwe
SLA	Service Level Agreement
TSA	Time Stamping Authority

1 About the Document

The primary goal of the document is to define the requirements for creating and launching Secure Data Exchange in Zimbabwe.

The information in the document is intended to be used when preparing the Secure Data Exchange Procurement.

Structure of the document:

- Background
- Objective
- Statement of Work.
- Tasks and Deliverables

External content references are used where possible to reduce the document's size and avoid duplication of the information.

2 Background

Data constitutes a key element of digital transformation, as every interaction in a digital setting generates data, and most depend on the availability of data in digital format. Developing a digital society requires governments to understand better what kind of data is available digitally both offline and offline, and how it can be aligned and used for creating value in the public sector and society.

Digitalisation of public services means ministries and government agencies capture and process data in machine-readable form. Digital transformation requires digital databases and data exchange between those. The modern digital governance model is a component-based service model, allowing the establishment of public services by reusing existing service components as much as possible.

Most of the respondents at OPC and MICTPCS view the legal framework as adequate for using electronic records and document management systems. In contrast, others feel the legal framework still has shortcomings and requires alignment. Furthermore, there is a need to set clear rules for the establishment of databases and interoperability of data.

According to the digital governance survey, using electronic records and document management systems and developing digital databases varies across government institutions. For instance, land and property registers and spatial information are not yet available in electronic format. Yet, the data in the population and business registers are partially available in electronic format. Moreover, ownership of data held by government authorities is not always clearly established.

Through MICTPCS, POTRAZ as the Data Protection Authority is assigned as the data governance institution, but a data governance and management strategy/policy does not exist yet. Data governance principles, including data management, data description, and data quality management, have not yet been adopted at the national level and across MDAs.

According to the respondents, a catalogue of state databases, services and other ICT assets has been partly implemented, but regular inventories are not always adequately carried out. Most digital platforms function in silos, and lack of interoperability limits collaboration and data sharing across government systems. The absence of a secure government data exchange tool is a pressing concern, as interviewees have identified it as a critical challenge. Currently, data is exchanged through manual, paper-based systems, underscoring the need to develop a secure digital solution for government data exchange. Furthermore, respondents also noted shortcomings regarding the supportive legislation for data exchange between government organisations and the reuse of digitised data within the public sector.

3 Objectives of RFP

The project's objective is to establish a Secure Data Exchange solution to support the implementation of the whole-of-government architecture.

The data exchange project must reach the following objectives:

1. Platform technical setup - establishing local instances of the platform for all necessary staging levels.
2. Deployment of an internal stack of PKI services.
3. Established platform organisation - defined standard operating procedures and maintenance routines for a local team.
4. Established monitoring for the data exchange platform and SLA.
5. Training of local experts – a task force for maintaining and managing the platform and supporting the implementation of integrations.
6. Launch of three to five pilot projects (in collaboration with service design framework) to demonstrate platform usability and improve some public services.
7. Documentation about the technical setup, the data exchange platform and description of operating procedures.

The project is expected to be delivered within six months with a competent partner and committed team. The full potential and effectiveness of the data exchange platform can be achieved together with services enabling the exchange of information between MDAs. Therefore, focusing on service design and digitalisation in parallel.

Zimbabwe's Government is looking for a vendor that has completed secure data exchange deployment projects in various countries of the world for at least the last three years. The contents of these projects have been the implementation of secure data exchange, integration support, training and consultations.

4 Statement of Work

1. The vendor will work with the Office of the President and Cabinet to establish a centralised Secure Data Exchange solution to facilitate a standardised exchange of data for the Government of Zimbabwe.
2. The vendor will work with participating Government of Zimbabwe ministries, departments and agencies as needed to complete the assignment.
3. The vendor will deploy a team of, at minimum:
    1. a Team Leader/Project Manager,
    2. an Interoperability Expert,
    3. a Data Exchange/ Infrastructure Expert,
    4. optionally other short-term or non-key professionals as needed to complete the assignment.

5 Roles and Responsibilities

1. The Office of the President and Cabinet will be the vendor's main counterpart and point of contact.
2. The Office of the President and Cabinet will appoint a Project Lead as the main focal point for to coordinate all project-related activities, manage resources, and ensure timely delivery of deliverables.
3. The Office of the President and Cabinet will establish an Oversight Committee for strategic leadership and direction of all project-related activities.
4. The Technical Team comprising experts from the vendor and selected local staff will implement the data exchange platform according to specifications.
5. The Office of President and Cabinet will arrange the allocation of necessary networking and server hosting environment for the Secure Data Exchange and PKI solutions.
6. The Team Leader will report directly to the Project Lead in the Office of the President and Cabinet and seek concurrence from that Office on key project deliverables before they are submitted to the Oversight Committee for concurrence, approval and sign-off to enable payment authorisation.
7. End users will provide input, feedback, and user testing throughout the project lifecycle.

6 Tasks and Deliverables

6.1 Task #1: Inception of the project

During this phase, the vendor's team will:

1. Agree on Project Management principles like communication channels, schedule for regular meetings, relevant contact information, failover- and escalation procedures, etc.
2. Create a list of key stakeholders.
3. Compile a detailed Project Plan.
4. Compile the list of Data Exchange and PKI-related procedures to be described and documented for the Data Exchange operator.
5. Describe the architecture and technical specifications for the Secure Data Exchange solution.
6. Describe hardware and environment requirements for deployment of the trust services.
7. Describe hardware and environment requirements for deployment of the Data Exchange servers.
8. Describe the configuration for the Data Exchange Platform and PKI servers.
9. Compile the documents with the information listed above.

Deliverable 1

Documents with all the information in the task list above (Task #1 Inception of the project).

6.2 Task #2: Deployment and configuration of PKI

During this phase, the vendor's team will:

1. Deploy and configure CA.
2. Deploy and configure TSA.
3. Test PKI services to verify they are working correctly.
4. Create documentation about the deployments made and details of configuration.

Deliverable 2

Deployed PKI services and corresponding documents.

6.3 Task #3: Deployment and configuration of the Data Exchange Servers

During this phase, the vendor's team will:

1. Deploy local mirror of the Data Exchange Repository.
2. Deploy production, test, and development environments of the following: Central server and associated components (e.g., central server security server, configuration proxy).
3. Deploy security servers for at least ten (10) Members that will share or consume data on the Data Exchange Platform.
4. Deployment and configuration must follow the guidelines as defined by the manufacturer or developer of the selected technology.
5. Test deployed servers to verify if data exchange between servers is working correctly.
6. Create documentation about the deployments made and details of configuration.

Deliverable 3

Fully functional Data Exchange Platform and corresponding documents.

6.4 Task #4: Established monitoring for the data exchange platform and SLA

During this phase, the vendor's team will:

1. Deploy and configure the data exchange platform's Monitoring modules.
2. Define SLA terms in cooperation with the Beneficiary's representatives.
3. Test the deployed modules to verify that the monitoring works correctly.
4. Create documentation about the deployments made and details of configuration.

Deliverable 4

Deployed Monitoring modules for the data exchange platform and corresponding documents.

6.5 Task #5: Description of operating procedures and maintenance routines

During this phase, the vendor's team will describe the:

1. Procedures and security guidelines for operating PKI servers.
2. Procedures and security guidelines for operating central servers for the data exchange platform.
3. Procedures and security guidelines for operating and monitoring the data exchange platform.
4. Procedures for updating software for the data exchange platform.
5. Procedures for the management of various instances of the data exchange platform.

Deliverable 6

Documents with procedures and security guidelines for items listed above.

6.6 Task #7: Training of local experts

During this phase vendor's team will:

1. Conduct training covering the following topic areas:
    a. operating of central servers,
    b. operating of security servers,
    c. operating of trust services,
    d. training service developers/integrators (train the trainer).

Deliverable 7

Training of local experts.

All training materials – presentations, training tasks.

6.7 Task #8: Pilot Services

During this phase, the vendor's team helps (consulting and guiding) the Beneficiary's team to:

1. Connect three to five services to the engine for secure data exchange.
2. Configure and test the consumption of these services from data consumers.

Deliverable 8

Documentation with the configuration of Member Security Servers used to connect Provider and Consumer Services to the data exchange platform.

6.8 Task #9: Evaluation and Monitoring of the Data Exchange Platform

During this phase, the vendors will:

1. Define criteria for evaluating the success of the project, including:
    a. Functionality, usability, and performance of the data exchange platform.
    b. Adherence to project timelines, budgets, and quality standards.
    c. User satisfaction and adoption rates.
2. Establish processes for monitoring progress, tracking milestones, and addressing issues or risks as they arise.

6.9 Task #10: Governance and Oversight

During this phase, and in conformance with governance elements defined in the Statement of Work, the vendor will:

1. Define governance structures and mechanisms for project oversight, decision-making, and accountability.
2. Establish reporting lines, communication channels, and escalation procedures for resolving issues and conflicts.
3. Identify key stakeholders who will be responsible for monitoring and evaluating project progress.

6.10 Appendices by OPC

Include any additional documentation or references relevant to the project, such as:

- Stakeholder analysis.
- Technical specifications.
- Risk management plan.
- Project management framework.

Delivering a seamless Government experience

D6-2

Requirements for Establishing Digital Identity for the Government of Zimbabwe

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

Glossary

Term	Definition
OPC	Office of the President and Cabinet, Zimbabwe
MDAs	Ministries, Departments and Agencies, Zimbabwe
ICT	Information and Communication Technologies
PKI	Public Key Infrastructure
CA	Certification Authority
TSA	Time Stamping Authority
SLA	Service Level Agreement
Digital Identity Token	Digital Identity Tokens are digital representations of a person's identity

1 About the Document

The primary goal of the document is to define the requirements necessary for creating and launching Digital Identity in Zimbabwe.

The information in the document is intended to be used when preparing the Digital Identity Procurements.

Establishing a strong governmental digital identity platform must be done in two phases. The requirements are, therefore, presented in two separate sets – one for each phase.

- Phase 1, Organisational setup
    - Task #1 - Inception of the project
    - Task #2 - Analysis of the current situation related to management of identity management
    - Task #3 - Development of digital identity system concept and management model
    - Task #4 - Describing architectural and technical requirements
    - Task #5 - Defining changes to existing systems and solutions needed for implementation of the digital identity solution
- Phase 2, Technical and organisational setup and launch
    - Task #6 - Digital identity token – vendor selection
    - Task #7 - Private Key Infrastructure deployment
    - Task #8 - Preparations and the start of issuing of digital identities
    - Task #9 - Integration of digital identity services with selected government services

Listed Tasks are divided between 3 (or 2) Procurements:

- Procurement #1 – looking for consultancy firm for Tasks #1, #2, #3, #4, #5, #8, #9
- Procurement #2 – looking for a vendor for Task #6
- Procurement #3 – looking for a vendor for Task #7

Important! Details of Procurement #2 and #3 will be defined during Phase 1.

In addition to stakeholder mapping and capability and needs assessment, the digital identity token selection (pre-condition for Task #6) requires analysis of techno-social limitations among subjects of digital identity to identify the most acceptable approach for the token.

The decision on whether to implement a PKI as a government service for all government services or to allow separate PKI services for Data Exchange and Digital Identity is the subject of investigation in Phase 1. A decision on this will also be made by the end of Phase 1 at the latest.

Procurement #2 and #3 can be combined into one procurement if the analysis during Phase 1 determines that this may be reasonable.

The current document is structured as follows:

- Background
- Overall Objectives
- Details for Phase #1:
  - The Objective of Phase #1 for Procurement 1
  - Statement of Work for Procurement 1
  - Tasks and Deliverables (Tasks #1- #5)
- Details for Phase #2
  - The Objective of Phase #2 for Procurement 1
  - Tasks and Deliverables (Tasks #8, #9)

External content references are used where possible to reduce the document's size and avoid duplication of the information.

2 Background

For digital governance services to be accessible, it is essential that the users can securely identify themselves and that the digital identity be strongly linked to how the identity of the Zimbabwean population is managed. This requires the development of the digital identity concept and tools. Digital identity is expected to allow future interaction and linking to electronic signature solutions.

The national identification system was implemented under the National Registration Act. In 1996, the Zimbabwe Population Registration System was created to contain all biographic personal data shared for digital governance. A unique persistent identifier of persons is implemented from birth, with 87.9% of the population enrolled, according to the Zimstats Population Census of 2022. Unique alien ID numbers are issued to foreign residents based on the nature of their residence permits. Records in National ID are stored in electronic format. Biometric IDs were introduced in the early 2000s.

While an e-identity system is not in place, citizens can access government e-services using the identification number from a national ID card - without electronic features or functionalities. Services are also available for foreign residents who have applied for their Alien ID. However, there are still other parallel identifiers in use, e.g. the national social security number. The most prominent identification methods for using digital government services include usernames and passwords, as well as mobile apps. A digital signature, along with its tools and supportive legislation, does not exist yet.

In the context of service digitisation, the absence of digital identity systems is seen as a significant hurdle. Currently, the identification and registration of users is predominantly a manual process, requiring individuals to present themselves at designated offices physically. For instance, the Ministry of Lands, Agriculture, Water, Fisheries & Rural Developments relies on Agritex offices in different districts to register farmers by collecting their physical ID documents. Similarly, the Ministry of Local Government & Public Works handles user registration and document verification through the assistance of the Civil Registry Department. Such reliance on manual procedures highlights a clear challenge in the transition to digital services, emphasising the need for an integrated e-identity framework to streamline and modernise these administrative processes.

3 Overall Objectives

The primary objectives of establishing a National Digital Identity system for the Government of Zimbabwe include:

1. Enhancing service delivery improves access to government services by providing citizens with a secure and convenient means of authentication for online transactions and interactions with Government agencies.
2. Strengthening security, and mitigating identity fraud, unauthorized access, and data breaches by implementing robust authentication and verification mechanisms that ensure the integrity and confidentiality of personal information.
3. Promoting inclusion and ensuring that all citizens, including those in underserved or marginalized communities, have equal access to digital services and can fully participate in the digital economy and society.
4. Facilitating interoperability to enable seamless integration between government systems and services, as well as with external stakeholders such as private sector entities and international organizations.
5. Fostering trust and confidence among citizens, businesses, and other stakeholders in the security and reliability of digital transactions and interactions with the government.
6. Supporting Economic Growth: To stimulate innovation, entrepreneurship, and economic growth by creating an enabling environment for digital businesses and fostering the development of digital ecosystems.
7. Empowering citizens with greater control over their personal data and digital identities, enabling them to exercise their rights and engage more effectively with government and other service providers.
8. Improving efficiency and cost-effectiveness by streamlining administrative processes, reducing paperwork, and eliminating duplication of efforts, leading to greater efficiency and cost savings for government agencies and taxpayers.
9. Supporting national development goals towards the achievement of broader national development goals, such as poverty reduction, social inclusion, and sustainable development, by harnessing the transformative potential of digital technologies.

4 Approach

Addressing the primary challenges related to digital identity expectations at the early stage of the process by creating a model for digital identity before the tangible digital identity elements are built and rolled out is crucial for a successful procurement process where the resulting digital identity would be usable in all necessary use-cases and scenarios. Zimbabwe is looking for the best suitable solution for a Digital Identity system. Crucially, the Digital Identity System must be designed with inclusivity, ensuring accessibility for all residents, regardless of their access to specific technologies, including those without smartphones. Moreover, paramount emphasis must be placed on implementing stringent security measures and the safeguarding of personal data, guaranteeing the highest levels of protection for individuals.

The ID document lifecycle is a pivotal element in a registry-based Digital Identity system, ensuring the integrity and functionality of the system throughout its operational lifespan. It encompasses the Digital Identity issuance, management, renewal, revocation, and retirement. This process not only supports the distribution and control of Digital Identity but also plays a critical role in data security and the preservation of citizen privacy.

Establishing a solid governmental digital identity platform must be done in two phases to ensure that the approach and solution implemented follow the requirements of the Government of Zimbabwe. Additionally, implementation in two phases reduces the risks of the whole implementation approach.

- **Phase 1, Organisational setup.** defining organisational roles for the identity ecosystem and refining the subjects. In this step, organisational relations, motivation and management model (covering relationships and responsibilities of stakeholders of the digital identity system) for the identity ecosystem are defined. It is important to carry out a study to identify techno-social limitations among subjects of digital identity to identify the best solution for the token (or even multiple tokens) for digital identity solution. Hasty and unsuccessful token selection hinders the adoption of a digital identity solution and has a broader impact on the government's digitisation plans. As a result of phase 1, a follow-up can be executed where digital identity tokens and systems are to be implemented (phase 2). The primary tasks of phase 1 are:
    - Task #1 - Inception of the project
    - Task #2 - Analysis of the current situation related to management of identity management
    - Task #3 - Development of Digital Identity system concept and management model
    - Task #4 - Describing Architectural and Technical Requirements

    - Task #5 - Defining changes to existing systems and solutions needed for implementation of the Digital Identity solution.
- **Phase 2, Technical setup and launch.** The second phase of the project implements necessary technical changes in stakeholder organisations and prepares identity document production, personalisation, and distribution pipeline. Ensuring that necessary security mechanisms are adopted and validated is critical. As an additional step, sometimes missed in some countries, technical tools and support measures for easier adoption for service providers must be put in place, and operations must be validated with some pilots. As part of this phase (and if required by the requirements), a stack of PKI services is to be established - this can be done as part of a Digital Identity project or as a separate foundational project combining PKI services from Data Exchange and Digital Identity. Timewise the decision to establish a dedicated PKI foundational project is therefore not critical and should be made by recognising risks related to the foundational project's implementation.
    - Task #6 - Digital Identity Token – vendor selection
    - Task #7 - Private Key Infrastructure deployment
    - Task #8 Preparations and Start of Issuing of Digital Identities
    - Task #9 - Integration of Digital Identity services with selected government services

Requirements for task #6, task #7, task #8 and task #9 are described as the result of activities in phase 1.

5 Phase 1

5.1 Phase 1 Objectives of RFP for Procurement #1

The project's objective is to establish a Digital Identity solution to support the e-Government services.

Zimbabwe is looking to boost its digital transformation by establishing a national digital identity. As the authorities and ministries have made their first steps toward digitalisation, the lack of a unified nationwide digital identity for citizens has been identified as the key barrier to faster digitalisation. This phase is time-sensitive, and OPC expects the partner organisation to engage and facilitate discussion on time. The phase must be completed within six months from contract signing.

As a result of Phase 1 of the Digital Identity project, the Zimbabwean government is expected to have a path, realistic expectations on the implementation agenda and required resources for establishing a Digital Identity solution. This would enable the continuation of the work for the provision of electronic services for the residents of Zimbabwe.

Zimbabwe's Government is looking for a partner who has completed digital identity implementation projects in various countries of the world for at least the last three years. The content of these projects must have included an analysis of the digital identity as-is situation and the description of the desired solution, planning of activities related to the implementation of digital identity, support of digital identity-related changes, and consultations.

5.2 Statement of Work for Procurement #1

1. The vendor will work collaboratively with the Office of the President and Cabinet to establish a Digital Identity solution for the Government of Zimbabwe.
2. The vendor will work with participating Government of Zimbabwe ministries, departments and agencies as needed to complete the assignment.
3. The vendor will deploy a team that consists of, at minimum, 1) a Team Leader/Project Manager, 2) a Legal Expert, 3) a Digital Identity Expert, 4) a Data Management Expert, and other short-term professionals as needed to complete the assignment.

5.3 Roles and Responsibilities for Procurement #1

1. The Office of the President and Cabinet will be the vendor's main counterpart and point of contact.

2. The Office of the President and Cabinet will appoint a Project Lead as the main focal point for to coordinate all project-related activities, manage resources, and ensure timely delivery of deliverables.
3. The Office of the President and Cabinet will establish an Oversight Committee for strategic leadership and direction of all project-related activities.
4. The Technical Team comprising experts from the vendor and selected local staff will develop and implement the Digital Identity solution according to specifications.
5. The Team Leader will report directly to the Project Lead in the Office of the President and Cabinet and seek concurrence from that Office on key project deliverables before they are submitted to the Oversight Committee for concurrence, approval and sign-off to enable payment authorisation.
6. End users will provide input, feedback, and user testing throughout the project lifecycle.

5.4 Task #1: Inception of the Project

During this phase, the vendor's team will:

- Agree on project management principles like communication channels, schedule for regular meetings, relevant contact information, failover- and escalation procedures, etc.
- Clarify intermediate and final deliverables for all activities.
- Compile a detailed Project Plan
- Compile the documents with the information listed above.

5.4.1 Deliverables

Documents with all the information listed in the task list above.

5.5 Task #2: Analysis of the Current Situation

In the initial phase of the project, input information for detailed analysis is carried out, identifying the baseline for defining a digital identity model. The outcome of this phase will describe different organizations involved in identity management and/or providing information about identity, including related regulations and processes. The goal is to ensure a thorough understanding of the existing landscape and regulatory framework, thereby laying a solid foundation for the project's subsequent stages.

5.5.1 Task 2.1 Organisational mapping

Organisational mapping is needed to get an overview of the organisations' functions, duties and dependencies related to identity management. This overview will include:

- Organisational processes related to identity registration, issuance and/or provision of identity information.
- Regulations give these organisations mandates and/or obligations or restrictions when dealing with identity management and/or providing identity information.

The overview will expose dependencies that will help in the next phase to select the best possible digital identity system concept and management model.

5.5.2 Deliverable 2.1

Document(s) with aggregated information about Organizational Mapping collected during this activity.

5.5.3 Task 2.2 Regulation and Process Analysis

This part of the analysis will be done in parallel with the "Organisational mapping" but with a focus on the identity management processes and their related regulations. The analysis report will describe the overall processes (cross-organisations) in the identity/identity document lifecycle. It also pinpoints regulations and requirements for these lifecycle processes.

This analysis will help in the following phases to find the best-suited (most efficient and secure, but with the slightest changes) Digital Identity system concept and it will be used as a baseline when defining changes needed in the last phase of this project.

During this activity, the following results will be delivered:

- An identity management and identity document-related regulation information collection for further analysis; will cover the set of regulations sent by the OPC and by using online information. This set of information will be used as core information for further analysis.
- Analysing part(s) of legislative acts that regulate identity management and identity documents: describing the scopes of different regulation acts, responsible organisation (s) and dependencies between the regulations while pinpointing specific articles.

The final analysis report will be used in phase 2 of this project as input information.

5.5.4 Deliverable 2.2

Document(s) containing systematised and aggregated information about Identity Management processes and regulations.

5.6 Task #3: Development of Digital Identity Concept and Management Model

This task aims to deliver a sustainable, cost-efficient, secure concept for the Digital Identity System with a management model. To achieve this, the input information from the previous phase must be delivered on time and with confirmed information accuracy.

All aspects of the current situation must be analysed to understand which organisations and process logic must remain and how the new system should adapt to possible constraints.

The analysis of the current situation must also include security and sustainability aspects of Digital Identity. For this, some best practices and international standards must be used as reference information of the digital identity.

During this phase, the consulting firm team will:

- Map current organisational functions, aligning them with best practices and standards to pinpoint what is covered, what can be covered, and what is missing in the current situation.
- Analyse local constraints and possibilities to define possible solutions for missing functionalities.
- Assess possible solution implementation impacts on economy and sustainability and pinpoint the most cost-efficient and sustainable approaches and technologies for addressing the identified functional deficits.

This project phase is time-sensitive due to the OPC's plans to start on time with the procurement process for the development of the Digital Identity system. Therefore, it is of high priority to have fast information exchange and communication between the shareholder's contacts and the consulting firm's team.

This phase will finish with the formal acceptance of the concept and management model by the OPC.

5.6.1 Deliverable 3

Documentation for the concept of the Digital Identity system and associated management model.

5.7 Task #4: Describing Architectural and Technical Requirements

This task is directly related to the OPC's procurement process for a new digital identity system. This task's output will be used in the procurement documents as the technical requirements are set.

When the concept and management model for the Digital Identity system is finalised (Task #3) and accepted by the OPC, the consulting firm's technology and security experts will define the technical architecture and related technical requirements for the system. These requirements will be structured in a way they would fit as a part of the procurement documentation for phase 2.

The architectural and technical requirements shall cover the following aspects:

- Centralised identity repository
- Card (or other token) general technical characteristics
- Card (or other token) security and protection
- Information and data exchange with the issuing authority
- Quality and functionality tests
- Digital Identity activation and revocation
- Recommendations for SLA and guarantees for procurement documents to ensure the quality of the service and timely delivery.
- Scalability of the Digital Identity System architecture for future technological advancements.
- Data privacy and compliance with industry standards and protocols for digital identity

In addition, consultant firm experts can suggest or advise the OPC about typical guarantees and SLA requirements.

5.7.1 Deliverable 4

Document with a list of requirements for technical development of Digital Identity solution and Recommendation of the implementation plan.

5.8 Task #5: Identify Necessary Changes to Implement the Digital Identity.

As a final part of Phase 1 of the project, the consultant firm's team will document changes that should be implemented to get the Digital Identity solution implemented. This task will use as-is information from Task #2 and define all gaps regarding the to-be situation defined in Task #3 (and in Task #4 if needed).

The scope of this documentation will cover only tasks/actions that the OPC should do within the government organisations and regulations.

The documentation provided as the result of this phase will be an input for the OPC to set up an action plan for the second phase - implementation of the Digital Identity solution.

5.8.1 Deliverable 5

The change management plan draft covers all the aspects listed above.

6 Phase 2

The project's objective is to establish a Digital Identity solution to support the eGovernment services.

Beneficiary uses the output from Phase 1 to implement all necessary changes in stakeholders' organisations and arranges procurement and deployment of the Digital Identity technical solutions.

The vendor offers supervision and consultancy services to assist the government in performing the activities needed to successfully launch the Digital Identity solution by:

- Assisting the government with performing the needed change management to successfully launch the Digital Identity solution. (Task #8).
- Assisting the government in selecting, integrating, and launching the services with Digital Identity integration. (Task #9).

The following chapters describe individual tasks expected as part of Phase 2 implementation.

6.1 Task #6: Digital Identity Token – vendor selection.

Part of separate procurement.

6.2 Task #7: Private Key Infrastructure deployment

Part of separate procurement.

6.3 Task #8: Preparations and start of issuing of Digital Identities

The task uses Deliverable 5 (Change Management Plan) as the primary input. The consultant firm is expected to consult and supervise the Beneficiary's team in the:

- Organisational changes
- Changes in working processes
- Changes in legislation
- Communication of changes
- Adopting Digital Identity technology

6.3.1 Deliverable 8

Successful launch of Digital Identity solution.

6.4 Task #9: Integration of Digital Identity With Selected Government Services.

The consultant firm is expected to consult and supervise the Beneficiary's team in the:

- Changes in technology solutions
- Organisational changes
- Changes in working processes

6.4.1 Deliverable 9

Successful integration of government services with the Digital Identity solution and successful launch of these government services.

D6-3

Development of the Service Design Framework and Capacity Building Programme for the Government of Zimbabwe

Project: An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Table of Contents

1 About the Document

The primary objective of the document is to define requirements essential for developing a robust Service Design Framework (SDF) for the Government of Zimbabwe as a part of the Zimbabwean Whole of Government Architecture (ZWoGA), together with piloting the framework for three projects.

MDAs' effective citizen-centric public service provision necessitates a well-defined framework and policy, outlining principles, rules, guidelines, and specific skills not commonly available in public sector organizations. By emphasizing clear processes, accountability and citizen-centricity, the platform seeks to improve public service outcomes, foster trust, facilitate sustainable and user-centric development in public services and lay the ground for improved outcomes in different indices measuring public service delivery.

Content of the document:

1. Background: Context for the Service Design Framework.
2. Current situation: A brief overview of the present circumstances, highlighting general challenges.
3. Expected tasks and outcomes: Description of expected activities and deliverables.
4. Timeline: Overview of expected timeline.

2 Background

There are no established central business process management rules for developing and monitoring public service delivery in Zimbabwe. Previously, the Public Sector Reforms and Performance Management Department coordinated public digital services. However, with the establishment of the E-Government Technology Unit, this responsibility has become a joint effort with the Ministry of ICT, Postal and Courier Services managing the back-end systems.

Challenges MDAs are facing today:

1. There is no unified approach to what constitutes a good digital service and how to design one.
2. There is a lack or deficiency of standards or unified principles.
3. All MDAs are acting in silos, and there is no knowledge sharing or networking.
4. MDAs lack skilled personnel with good knowledge of service design.
5. The concept of service ownership is missing.
6. There is no clear understanding of how many services the Government offers and unclear delivery models.
7. Risks of not having a government-wide SDF

General information about public services is relatively accessible via government website(s). The key sites include the Central Government Portal[1], which provides access to all the government entities' websites. The Government established a guideline for developing and managing the Government of Zimbabwe's websites and Portals in 2018.

The Central Government Portal also includes the ZimConnect portal, which serves as a one-stop-shop for e-services delivered by the ministries, departments, and agencies. Helpdesk services related to public services have been partly implemented, and some campaigns have been held to ensure all citizens are aware of governmental digital solutions and related topics.

Coordination and standardization of digital public services development and management on a central level has just started, and there are no central business process management rules in place yet for the development and monitoring of public services. Also, there is no catalogue where all provided public services are listed. Each MDA has its processes and practices in place and a central approach to service design together with tools, knowledge sharing, and training is missing.

[1] https://zim.gov.zw

3 Objectives of RFP

The objective of the project is to develop a Service Design Framework for the Government of Zimbabwe supporting MDAs during the digital transformation process. The framework must include:

1. **Methodology** guidelines, recommendations, and a common set of requirements for designing, redesigning, and developing.
2. **Tools necessary for public service design,** service mapping, description, visualization, monitoring, assessment, project preparation etc.
3. **Training materials and environment for the MDAs (e-learning platform)** supported by creating a knowledge base, Training-of-Trainer and capacity-building programs.
4. **Piloting of SDF in 3 sample projects** (described in task 5)**.**
5. **Empowerment of persistent task force** acting as trainers and supporting digitalization of different public services if different MDAs and support establishment of an SDF Centre of Excellency.

The key beneficiary and client will be the E-Government Technology Unit under OPC. Capacity building activities, development of online courses etc. will be done in cooperation with the Public Service Commission.

The Service Design Framework is intended for the following target groups (initial list, not limited to):

1. The Public Service Commission is the key beneficiary of the digital transformation of public services.
2. Public Sector Reforms and Performance Management Department
3. Public officials engaged in the projects of designing and developing digital public services at both executive and administrative levels (services, G2B services etc.).
4. Public officials are responsible for change management and capacity building.
5. The Ministry of Information and Communication Technology, Postal and Courier Services.
6. M & E department

Selecting the final list of beneficiary organizations is the responsibility of the OPC, keeping in mind that the OPC's main function is leadership and coordination.

4 Statement of Work

1. The vendor will collaborate with the Office of the President and Cabinet to develop Service Design Methodology and tools for public service design. Additionally, they will create an online training environment and materials for the Government of Zimbabwe.
2. The vendor will work with participating Government of Zimbabwe ministries, departments and agencies as needed to complete the assignment.
3. The vendor will deploy a team that consists of:
    a. Team Leader/Project Manager
    b. Service Design/Content Expert(s)
    c. e-Learning Designer
    d. UI/UX Designer
    e. Quality Assurance Specialist
    f. Developer(s)
    g. Change Management Expert
    h. Capacity Building Expert
4. The Vendor may have other short-term professionals needed to complete the assignment.
5. The Office of the President and Cabinet will be the vendor's main counterpart and point of contact.
6. The Office of the President and Cabinet will appoint a Project Lead as the main focal point for all project-related activities.
7. The Office of the President and Cabinet will establish an Oversight Committee for strategic leadership and direction of all project-related activities.
8. The Office of the President and Cabinet will organize the provision of essential facilities for the development of the Service Design Framework, including stakeholder engagement, necessary seminar rooms and catering for relevant events.
9. The Team Leader will report directly to the Project Lead in the Office of the President and Cabinet and seek concurrence from that Office on key project deliverables before they are submitted to the Oversight Committee for concurrence and payment authorization.

5 Tasks and Deliverables

5.1 Task #1: Development of Service Design Methodology

The methodology shall include guidelines, recommendations, and a common set of requirements for designing, redesigning, and developing digital public services. The OPC and the Taskforce will oversee methodology in the future. The task force will utilize this methodology to support MDAs embarking on their digitalization journey.

During this phase, the Vendor's team must:

1. Identify goals and principles from the digital transformation approach of Zimbabwe and how these must be related to the development of integrated public services.
2. Describe the service design process with at least the following items:
    a. Principles to which integrated public services must comply (service design standard).
    b. Recommendations and examples of how to identify and describe user needs.
    c. Description of how to prepare and conduct user research.
    d. Methods and tools for needs and requirements analysis.
    e. How to design and prepare development projects, how to prepare procurement, and how to manage development projects (how to implement an agile approach).
    f. Minimum Viable Product (MVP) development approach.
    g. Design samples.
    h. How to choose service provision channels.
3. Analyse existing guidelines, and legislation and make recommendations for adjustments if needed.
4. Describe the development process.
5. Describe user-research methodologies.
6. Describe the minimum skills of MDA teams responsible for integrated public service development and management.
7. Define service delivery standards to ensure consistency and quality.
8. Describe data digitalization principles.
9. Describe data management principles.

Requirements for the Service Design Framework:

1. The framework must be logical and simple.
2. All texts must be in good and clear English and as short as possible.

3. The presented information must be formalized on a harmonized template, easy to use and practically implemented.
4. The framework must be easy to update.

5.1.1 Deliverables under Task 1

Guidelines, recommendations, and requirements for the development of integrated public service provision.

5.2 Task #2: Toolbox for Public Service Design

Tools for public service design support MDAs in service mapping, description, visualization, testing, monitoring, assessment, project preparation, etc. The selection of tools recommended for the public sector for designing digital services will support the service design process.

During this phase, the vendor's team must:

1. Describe the steps necessary for designing integrated public services through the service lifecycle.
2. Conduct interviews with at least 5 potential users of the future toolbox to identify the needs and expectations. The list of interviewees will be agreed upon later.
3. Describe activities needed for service mapping and suggest proper tools for such activities together with user guides for such tools.
4. Describe how business processes and use cases (AS-IS and TO-BE) should be described and suggest suitable tools together with user guides.
5. Describe how business requirements should be described and managed and suggest suitable tools together with user guides.
6. Describe methods and tools for user research.
7. Describe methods and tools for user testing.
8. Describe the prototyping process and suggest proper tools for prototyping.
9. Develop or suggest tools for effective performance management to monitor and assess the performance of public services.
10. Describe how to measure service quality and user satisfaction (incl. dev of KPIs).
11. Develop example SLAs.

Requirements for the toolbox:

1. The toolbox must be logical and simple.
2. All texts must be in good and clear English and as short as possible.
3. The presented tools (methods, canvases, instructions, etc.) must be formalized on a harmonized template, easy to use and practically implemented.
4. The toolbox must be easy to update.

5. Open-source software should be preferred when recommending tools.

5.2.1 Deliverables under Task 2

1. Toolbox for public service design service mapping, describing, visualizing, monitoring, and assessment.
2. User guides for public service design toolbox.
3. Example SLA template.

5.3 Task #3: Knowledge Base and Training Environment

During this phase, the vendor's team will:

1. Develop a technical solution - the Knowledge Base" - where deliverables of tasks 1 and 2 are published and made available to all MDAs.
2. Develop a clickable prototype of the knowledge base and test its initial content with up to 10 potential users to validate its understandability and applicability.
3. Deliver training, consultations, mentoring, and other capacity-building programs for up to 10 potential task force members.
4. Provide training, consultations, mentoring, and other capacity-building programs for the learning environment administrators (minimum of 2 persons) to independently maintain and manage the training environment.
5. Implement the Train of Trainer (ToT) approach to assemble a proficient team supporting MDAs in the adoption process.
6. Produce a 3-minute promotional video introducing the knowledge base and other activities and organize an outreach event for up to 150 participants to introduce its content.
7. Create promotional materials (e.g., one pager) to promote developed content.
8. Develop a clickable e-learning platform prototype.
9. Develop the e-learning platform and create five online courses for MDA officials about public service design and development covering the following aspects but not limited to:
    a. Introduction of ZWoGA.
    b. Overview of design and development process.
    c. Involving users in the design development of integrated public services.
    d. Introduction of data management.
    e. Introduction of secure service design and development.
10. Develop online courses with self-assessment tests and feedback forms for trainees.

Requirements for the online training environment:

1. The technical solution for the knowledge base and e-Learning Platform must be web-based. The landing page for the knowledge base and e-learning Platform must be the same.
2. The user must make as few clicks as possible to find the necessary information.
3. The clickable prototype must be created with the help of design software(s), which allows the creation of complete workflows in desktop, tablet and mobile view using clickable high-fidelity screen images (e.g. Figma).
4. The user interface must be accessible and meet at least WCAG 2.1 level AA.
5. The user interface must be compatible with the following web browsers: Chrome, Safari, Firefox and Microsoft Edge.
6. The user interface must be fully compatible with current HTML5, CSS3 and JavaScript standards and with all required web browser versions.
7. The user interface of the application must adapt to different screen views (computer, tablet and mobile phone).
8. The website must support several languages, and there must be an option to add other languages.
9. The technical solution must be Wiki-like indexed with search functionality, which also considers the addition of subsequent content topics to the web platform at a later stage of development.
10. Online courses and e-learning platforms must:
    a. Be interactive and enable the use of text, videos, photos, external and internal links, knowledge tests and feedback forms.
    b. Create and maintain motivation in the learner.
    c. To be learner-centred, the learning experience must be designed with e-learning in mind, and the learning journey must be described, including the learner's ability to understand the progress of their learning.
    d. Include short "learning sessions", repetitions, interactive content, self-monitoring and assessment activities with automatic feedback, and multimodality.
    e. Take the learner approx. 45-60 minutes to complete and consist of short up to 10-minute lessons that form a whole (for example, micro-learning as part of macro-learning).
    f. Include self-checking and evaluation activities that provide automatic feedback across all learning outcomes, interactive activities and/or visual materials (videos, animation, graphics) to keep the learner motivated, practice skills, reflect, etc. and references to more in-depth material or course(s), tests with feedback.
    g. Include knowledge tests and enable the issuing of certificates for participants. Allowed response types: multiple choice, open answer, drag-and-drop response, etc.
    h. Allow version management of courses.

i. Enable the administration of user groups, access rights, etc. This also applies to the knowledge base.
j. Enable creating courses based on modules.
k. Enable separate administration of platform and courses.
l. Include statistic module based on courses, individuals, MDAs and users.
m. Availability and access requirements are to be clarified.
n. Enable 100 users to take courses and tests at the same time.

11. All courses for public officials should be designed in English.
12. ToT program must include topics like the introduction of ZWoGA, an overview of the design and development process, involving users in the design development of integrated public services, introduction of data management, and introduction of secure service design and development.
13. ToT program must involve the training of seven specialists, including the training environment administrators.

5.3.1 Deliverables under Task 3

1. Training materials and e-learning platform for the MDAs (5 courses).
2. The ToT program is designed and executed for up to 7 persons.
3. Promotional video and materials.
4. Outreach event.
5. Development of a clickable prototype and fully functional online learning environment.

5.4 Task #4: Empowerment of Persistent Task Force

A persistent task force, operating under OPC guidance, will serve as trainers and support public service digitalisation in different MDAs. The task force members are part of the Training of Trainers program.

During this phase, the Vendor's team will:

1. Empower the assigned task force supporting beneficiaries throughout the service digitalisation enhancing the skills and knowledge of task force members during the project. The task force is staffed by OPC, and other specialists drawn from relevant MDAs as shall be determined comprising:
    a. Business analyst
    b. Service owner
    c. Technical Architect
    d. UX Specialist
    e. UI designer

f. Legal expert
g. Training environment administrator.

2. Provide ongoing support from the task force throughout the transition period for up to 120 hours.

5.4.1 Deliverables under Task 4

Consultation and capacitation of the task force during the transition period.

5.5 Task #5: Pilot Projects

Service Design Framework must provide practical support to MDAs. Therefore, it is important that the framework is tested and that the experience received from pilot projects is described as part of the framework. Testing should be conducted in collaboration with MDAs.

During this phase, the vendor's team will:

1. Agree on three services which will be piloted using the Service Design Framework.
2. Conduct and document piloting according to the methodology developed in Task 1.
3. Support service owners during the procurement and development process for up to 100 hours.
4. Supervise development projects for up to 200 hours.

5.5.1 Deliverables under Task 5

The execution and documentation of piloting, aligned with the methodology formulated in Task 1, are accepted by OPC and MDAs.

Delivering a seamless Government experience

ZIMBABWE

An Enterprise Architecture Modelling Exercise for the Government of Zimbabwe

Published by: e-Government Technology Unit
Office of the President & Cabinet
Harare.
2024