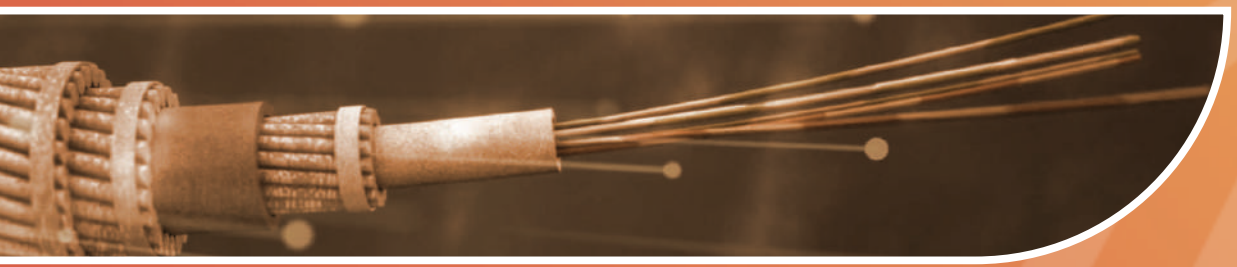
Papua New Guinea

PNG DIGITAL TRANSFORMATION POLICY



Published by
Department of Information and Communications Technology

P.O. Box 85
Vision City - Waigani
National Capital District
Papua New Guinea

www.ict.gov.pg

September 2020

ISBN: 978 - 9980 - 910 - 80 - 6

FOREWORD

This Policy is a high-level document that articulates the Government's thinking for Papua New Guinea's digital transformation. It documents our aspirations for unpacking and delivering digital infrastructure, digital government, digital skills, innovation and entrepreneurship, digital cyber security and privacy, and financial inclusion across the whole-of-government and sub-nationally.

Following National Executive Council (NEC) approval of a roadmap in 2018, work on developing the full policy document did not begin until 2020. The Department of Information and Communications Technology (DICT) under the leadership of Acting Secretary Steven Matainaho has done well in maintaining momentum and giving us an opportunity to appreciate the utility of information and communications technology (ICT) at a time when the government requires public expenditure savings and to extend the reach and raise the quality of the public service in Papua New Guinea (PNG).

We have heard stories of governments abroad that have recognized and successfully adopted and implemented ICT solutions to make public administration more effective and efficient, and we are excited. Countries such as Estonia, South Korea, the United States, Australia, and New Zealand have each achieved a certain degree of success with individual digital transformation and digital government programs. Their individual stories have inspired us, and we too seek to benefit from the same efficiencies and savings to ultimately benefit PNG and her people.

As a government, we are committed to progressing digital transformation and to making it a cornerstone of public administration. We want people in our rural communities to have the means to access government goods and services through mobile phones at minimal or zero cost and without the expense and wasted time of travel and queues. This is a dream that we as a government are keen on realizing by 2022 and we are convinced that we can realize this dream on the back of ICT, and the Internet.

I thank the DICT management and staff for putting this document together. I also acknowledge the input of various Social Law and Order Sector agencies, the Papua New Guinea Computer Society Inc., the PNG Digital Information and Communications Technology (ICT) Cluster Inc., and various peer reviewers both in-country and overseas for going through the policy and providing valuable feedback.

This Policy is now the apex policy for the ICT sector after receiving NEC approval[1]. And while it gives specific focus on public sector transformation across the whole-of-government, this is simply because the digital transformation journey must start from within.

It is imperative that this Policy be anchored under an appropriate overarching legislation. Additionally, all prior ICT relevant or referenced policies, national and sub-national, will require review and alignment to this overarching Policy.

I hereby present this Policy to the DICT, all other government agencies, development partners and industry stakeholders and look forward to your support in translating this Policy into successful programs and projects that will positively transform the livelihood of our people.

God bless you all,

Hon. Timothy Masiu, MP
Minister for Information & Communication Technology
4th September 2020, Port Moresby.

1 NEC Decision No. 252/2020 (26 August 2020).

EXECUTIVE SUMMARY

The Government of Papua New Guinea (GoPNG) is using digital transformation to change public administration processes, culture, and citizen experiences using information and communications technology (ICT) advancement as an enabler.

GoPNG is also focusing on implementing the Asia-Pacific Economic Cooperation (APEC) main priorities agreed to in 2017 under the theme "Harnessing Inclusive Opportunities, Embracing the Digital Future," to empower workers and businesses to change.

The APEC's 2018 priorities include:

- Improving Connectivity, and Deepening Regional Economic Integration;
- Promoting Inclusive and Sustainable Growth, and;
- Strengthening Economic Growth through Structural Reform.

In 2018, the National Executive Council (NEC) endorsed the ICT Sector Roadmap 2018 and approved the establishment of both the Ministerial Committee on ICT, and National ICT Sector Coordinating Committee to lead the process of digital transformation starting with digital government[2].

The Department of Information and Communication Technology (DICT), as the lead agency, aims to facilitate this transformation journey starting with transformation of government service delivery on a Whole-of-Government basis.

The digital transformation process envisions agencies and departments delivering a range of initiatives to improve inter-agency collaboration, that in turn should translate to improvement in public sector service delivery, through the use of innovative and more advanced ICTs.

Digital transformation promotes "digital experience" and will result in, among other things: standard operating environments to guide procurement of computing equipment; trusted digital authentication and authorisation services; whole-of-government platforms; electronic grants administration; and a streamlined online business registration service.

The digital transformation agenda will strive to put people first by:

- Fostering excellence;
- Empowering its employees;
- Promoting technology neutrality;
- Helping people solve their own problems, and;
- Cutting red tape.

It will do this by:

- Creating a clear sense of mission;
- Prioritising incentives over regulations;
- Delegating authority and responsibility;
- Setting open standards and frameworks for planning, implementation and assessment;
- Promoting collaboration and sharing of best practices;
- Adopting a competitive mindset;
- Searching for market, not administrative solutions, and;
- Measuring our success by customer satisfaction.

2 NEC Decision No. 289/2018 (12 October 2018).

This Policy

The transition to digital government starts with a transformation of the leadership mindset and vision for what government is and how it behaves, both internally and as it interfaces with its citizenry. It involves fundamental organizational change and the design of government programs rethought for a digital era. Digital government requires public policy makers and business leaders to collaborate to understand how ICT can be utilised to realise a digital government vision and it requires the government to muster the political will to reform accordingly.

This Policy sets out the benefits of digital government for civil society, the GoPNG, and the private sector, and draws attention to linkages to other international and national supraordinate policies. It provides a definition of digital government and explains some of the different models that can be adopted by GoPNG, but advocates for a Whole-of-Government approach and shared services for particular common functions so as to avoid duplication of and wasting of limited resources.

A list of the considerations made when writing this Policy is set out, particularly, that digital government starts with digital identity of legal and "digital" persons. Legal persons include businesses and natural persons, and a "digital" person corresponds to machines, computers, and applications that operate in digital environments.

A nuanced explanation of digital identity (ID) is given, so that the difference between functional and foundational ID can catapult development by permitting private sector consortiums to solve identification problems in harmony with whatever shape the national identification program takes in the future. A trustworthy digital identity and the domains of privacy and trust are inseparable.

A strategic framework is laid out and the scope of this Policy is organised into the following themes:

- Enabling the PNG people to access high-quality digital government information and services anywhere, anytime, on any device;
- Ensuring that as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways, and;
- Unlocking the power of government data to spur innovation across our country and improve the quality of services for the PNG people.

The policy focuses the actions and resources of various stakeholders, and particularly the government, on national ICT-enabled development priorities.

CONTENT

ACRONYMS

APEC	Asia-Pacific Economic Cooperation
DCIT	Department of Communication and Information Technology
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
G2E	Government to Employee
GoPNG	Government of Papua New Guinea
ICCC	Independent Consumer Competition Commission
ICT	Information and Communications Technology
IdSP	Identity Service Provider
ISP	Internet Service Provider
IGIS	Integrated Government Information System
IXP	Inter-Exchange Point
KYC	Know Your Customer
LLG	Local Level Government
MCICT	Ministry Committee on ICT
MRZ	Machine-Readable Zone
MTDP	Medium Term Development Plan
NDC	National Data Centre
NEC	National Executive Council
NICTA	National ICT Authority
NISIT	National Institute of Standards and Industrial Technology
NSDS	National Strategy for Development of Statistics
OOP	Once-Only Principle
OECD	The Organisation for Economic Co-operation and Development
PC	Personal Computer
PII	Personally Identifiable Information
PNG	Papua New Guinea
PWDs	Persons With Disabilities
ROI	Return on Investment
SDG	Sustainable Development Goals
SOE	State-Owned Enterprise
STaRS	National Strategy for Responsible Sustainable Development for Papua New Guinea
UN	The United Nations
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WCAG	Web Content Accessibility Guidelines
WSIS	World Summit on the Information Society

1. POLICY CONTEXT

1.1 Introduction

This document sets out the strategic framework for digital transformation within PNG's government business and the sector as a whole. It further provides the context, objectives, and scope, and issues concerning the implementation, monitoring and evaluation.

Digital transformation, in this context, means the integration of digital technology into all areas of the ICT sector, with specific focus on government business and public sector functioning, fundamentally changing how public services operate and deliver value to its citizens. Digital transformation implies changes to both technology and to institutional culture, and such changes that require organizations to continually challenge the status quo, to experiment, and to be prepared to sometimes learn from failure in the quest for the greater good.

Digital technologies—the internet, mobile phones, digital devices and all the other tools to collect, store, analyse, and share information digitally—have steadily integrated into the everyday lives of Papua New Guineas, businesses and government. Digital technologies make routine, transaction-intensive tasks dramatically cheaper, faster, and more convenient, and are here to stay. Papua New Guinea in its digital transformation journey, has the opportunity to leapfrog, through learning other countries' successes and experiences. For example, in Estonia a citizen's tax return is pre-filled and can take as little as 3 minutes to complete with a single
button click. Estonia cites that more than 16,400 person-years of work are saved each year from their digital transformation and automation – in other words, they can deliver the same quality of services and redeploy 16,400 to better and higher value work in government3.

World Bank studies have shown the impact of the Internet, the growth of mobile phones, and related technologies has a significant impact on economic development. A World Bank study concluded that a 10% point increase in broadband penetration would increase GDP growth by 1.38% in developing economies and 1.21% in developed economies. The same study found that after the introduction of broadband GDP per capita growth was 2.7% to 3.9% higher than before broadband. For fixed broadband the percentage increase of GDP per capita was higher and every 10 percent increase in fixed broadband penetration led to an average increase of 3.19% in per capita GDP.

GoPNG has recognized the significance of harnessing ICT to transform public administration ever since the introduction of the internet to PNG in 1997. However, there is room for improvement, and the timing is perfect, now that ICT has become a critical enabler of the "new normal" post COVID-19 activities of government, businesses and consumers. Enabling holistic and coordinated transformation of public administration by all government entities on the back of ICTs will result in efficiencies and achievement of sustainable development
goals at the national and subnational levels. This is the challenge the GoPNG is facing and one that it plans to meet head on.

1.2 Benefits of Digital Government

Digital government will contribute to economic and social development by transforming the country into a competitive, innovative knowledge-based society through:

- Increasing the quality of government service delivery;
- Increasing access to and sharing of information;
- Allowing for better use of government infrastructure and resources;
- Improving governance;
- Improving service delivery;
- Increasing efficiency and effectiveness;
- Enhancing the participation of private sector;
- Increasing transparency, and accountability;

3 Minges, Michael. Exploring the Relationship between Broadband and Economic Growth, Background Paper prepared for the World Development Report 2016: Digital Dividends, Jan. 2015.

- Reducing opportunities for corruption, and;
- Lowering costs.

Promoting and encouraging digital government will allow the government departments that support and encourage e-Government services and applications to be seen as leaders and innovators in the country.

Digital government systems can automate many paper-intensive and transaction-intensive tasks, but appropriate digital skills training is required to realize improved efficiency, equity, and access.

Digital government depends on empowering and motivating public servants to engage in major change and innovation and to collaborate in improving processes, systems, and programs.

Digital government also requires collaboration with the private sector in the establishment of digital government services and applications that reduce transaction costs and significantly improve performance.

ICTs are one of the key enablers to achieve these targets aiming at ensuring equal rights to economic resources, especially for the poor and the vulnerable, as well as ownership and control over different forms of property. ICT-related initiatives provide timely and accurate information services. They allow people to access the available economic resources they need to be equipped with skills and competencies. Capacity building, including digital skills development plays a central role, ensuring that ICTs are integrated in education and training at all levels.

Sustainable Development Goals (SDGs) targets define high-level objectives to which governments systematically align their development goals. To maximize Return on Investment (ROI), PNG needs to draw a line connecting its national development goals to the programmes it is implementing to achieve those strategic goals, and to connect each programme to the reusable software components which help deliver them.

A whole-of-government approach to digital transformation will allow PNG to not only achieve the SDGs but will also benefit the entire economy. By reducing information costs, digital technologies greatly lower the cost of economic and social transactions for firms, individuals, and the public sector. Digital technologies promote innovation when transaction costs fall to essentially zero. They boost efficiency as existing activities and services become cheaper, quicker, or more convenient. And they increase inclusion as people get access to services that previously were out of reach.

Taking a whole-of-government approach by looking at the impact of consumerscitizens, businesses, governments, and their partners by reducing costs and increasing efficiency will make the Government work better and cost less. By investing in reusable tools to build new applications and new services will increase efficiency and deliver a better ROI to all parties. These reusable building blocks and a focus on collaboration and innovation will also help create a platform ecosystem which in turn will provide incentives for application developers to develop new and innovative applications and services that can benefit all parties. Combining functionality in this way will attract increased investment which will, in turn, provide incentives for the private sector to fill the emerging cross-sector market demand and, critically, to extend services to populations that would not otherwise be able to afford them. Citizens or any consumer, who are the direct beneficiaries of ICT-supported programmes, will enjoy more integrated, comprehensive, and higher quality services from their government, ultimately leading to improved livelihoods based on the premise that:

- ICT has been recognized as cross-cutting across all sectors of the economy;
- ICT is a key driver and enabler of enhanced efficiency, effectiveness, and transparency in public service delivery;
- The Sustainable Development Agenda was adopted by the UN in September 2015 and has 17 Sustainable Development Goals (SDG);
- Expansion of e-Government services is a driver of demand for ICT and provider of affordable access

directly or indirectly, and;
- e-Government applications and services ensure responsive, inclusive, participatory and representative decision making at all levels--as stated in Goal 16 of the SDGs.

1.3 Policy Alignment

This Policy is aligned with national development goals and other policies in the following ways.

1.3.1 PNG Vision 2050

- Vision 2050 envisions increased communication access from 10% to 100%
- Establishment of a communications satellite network for PNG
- Establishment of a National Information Database Management System

1.3.2 Long Term Development Strategy 2010-2030

- A modern and affordable information and communications technology system that reaches all parts of the country
  - 800 mobile subscribers per 1,000 people by 2030
  - 70% of the population have access to or use the internet by 2030
  - 100% of Papua New Guineans must have access to radio and television by 2030

1.3.3 Alotau Accord III (2017)

- 2 out of 85 priorities
- Recognises ICT as key enabler for development of PNG
- Completion of the national fibre-optic cable infrastructure
- Delivering e-commerce, e-health, e-agriculture and e-government

1.3.4 Medium Term Development Plan III 2018 - 2022

A total of 11 provinces connected to Integrated Government Information System (IGIS) National Data Centre (NDC) and access its shared services by end of 2019, and by 2022 will connect 22 provinces to the NDC.

1.3.5 National ICT Policy 2008

The National ICT policy sets out a strategic framework for meeting the Government's objectives for the ICT sector. Under this Policy the Government reaffirms its commitment to the staged introduction of open competition in the telecommunications sector and the transformation of Telikom PNG into a viable and efficient retail competitor in the market.

The Government will revise and realign the National ICT policy with this Policy, as much has changed in the 12 years since it was published, and digital transformation of the public sector, civil society and the private sector will be dependent on an efficient, dynamic, and competitive retail market for telecommunications services.

1.3.6 PNG Strategy for the Development of Statistics 2018-2027

National Executive Council (NEC) Decision No. 135/2010 highlighted the lack of core statistics needed in today's economy for informed decision-making and evidence-based planning. It directed relevant Government departments responsible for producing and using statistics to develop a National Strategy for the Development

of Statistics (NSDS) for the country. It developed data sets on climate, land, biodiversity, coastal and marine life, water, and culture and heritage.

The NSDS is designed to strengthen the PNG statistical system and supports PNG's development agenda by fostering greater use of evidence in policy making and development planning. It is a cycle that will have two midterm reviews before a major review in 2027.

1.3.7 APEC 2018 Chair's Era Kone Statement

This Policy gives effect to the APEC 2018 Chair's Era Kone Statement, including the delivery of APEC Bogor Goals, and the Individual Action Plan.

Relevant in the Roadmap and addressed broadly in this policy are;

- Digital Infrastructure;
- Promotion of Interoperability;
- Achievement of universal broadband access;
- Development of holistic government policy framework for the Internet and Digital Economy;
- Promoting coherence and cooperation of regulatory approaches affecting the Internet and Digital Economy;
- Promoting Innovation and adoption of enabling technologies and services;
- Enhancing trust and security in the use of ICTs;
- Facilitating the free flow of information and data for the development of the Internet and Digital Economy, while respecting applicable laws and regulations;
- Improvement of baseline internet and Digital Economy measurements;
- Enhancing inclusiveness of the Internet and Digital Economy; and
- Facilitation of e-commerce and advancing cooperation through Digital Trade.

1.3.8 National Security Policy 2014 and the National Security Policy Strategic Action Plan 2014-2020

This policy gives effect to the National Security Policy (NSP) and National Security Policy Strategic Action Plan (NSP SAP) 2014-2020, and in particular; Policy Goal eight of NSP SAP which focuses on 'Ensuring Technological Security'.

The NSP calls for every relevant agency to understand the inextricable links between security and development, and ensure institutional frameworks and action plans link with the NSP framework so that they support and contribute to the NSP agenda.

1.3.9 Draft 2017 National Intellectual Property Strategy

The Draft 2017 National Intellectual Property Strategy is the GoPNG 10-year development strategy that supports science-based technological development and innovation in the areas of business, processing, the environment, services and health on the back of intellectual property rights.

1.3.10 Sustainable Development Goals

The UN's Global Development Agenda for the period 2015-2020, known as the Sustainable Development Goals (SDG), comprises 17 goals and 169 targets that span across all sectors, including elimination of poverty and hunger, environmental protection, sustainable economic development, sustainable cities and communities, and institutional development. In turn, each country, including PNG considers the SDGs in its national priorities.

The WSIS process has identified digital lines of action and targets for all sectors. For example, e-agriculture

has a great potential to ensure the availability of information to all, to increase networking and partnership, and to raise awareness on sustainable development. PNG has taken significant steps towards e-agriculture adoption. It also supports information gathering, analysis, planning and supply systems, necessary for nutrition information and interventions to be delivered

For ICTs to play a central role, policies and regulations must contribute to reducing barriers to broadband development; facilitate build-out of national fibre-optic networks and international connectivity links. SDG goal 9 speaks about building resilient infrastructure and promoting inclusive and sustainable development and fostering innovation. It is this SDG goal where much of the connectivity, ICT, and many digital government initiatives fall within.

One of the main objectives of this goal is to provide universal affordable access to the Internet for all citizens, and to support local governments in strengthening their capacity and improving their service delivery.

The WSIS Action Lines were the UN's Framework used to implement the Millennium Development Goals (2000-2015) and now they are used to implement the SDGs (2015-2030).

1.4 Definition, Nature, & Types of Digital Government Service

1.4.1 What is Digital Government?

Digital government is the use of ICT to improve the efficiency and effectiveness of public sector operation and service delivery; or alternatively, the use by governments of ICTs to transform relations with citizens, businesses, and within government. Digital Government promotes and improves stakeholder contributions to development, as well as deepens the governance process.

The Organisation for Economic Co-operation and Development (OECD) defines it as the use of new ICTs by governments as applied to the full range of government functions[4]. In particular, the networking potential offered by the Internet and related technologies has the potential to transform the structures and operation of government.

The European Commission[5] defines it as the use of digital tools and systems to provide better public services to citizens and businesses. Effective e(digital)-Government can provide a wide variety of benefits including more efficiency and savings for governments and businesses, increased transparency, and greater participation of citizens in political life.

ICTs are already widely used by government bodies, as it happens in enterprises, but e-Government involves much more than just the tools. It also involves rethinking organisations and processes and changing behaviour so that public services are delivered more efficiently to people. Implemented well, e-Government enables citizens, enterprises and organisations to carry out their business with the government more easily, more quickly and at lower cost.

The World Bank defines *digital government*[6] as processes that:

- Makes routine, transactions-intensive tasks significantly cheaper, faster, and more convenient;
- Promotes efficiency;

4 Online source: https://www.oecd.org/governance/digital-government/toolkit/12principles/, accessed: 12 May 2020.

5 Barcevičius, E., Cibaitė, G., Codagnone, C., Gineikytė, V., Klimavičiūtė, L., Liva, G., Matulevič, L., Misuraca, G., Vanini, I., Editor: Misuraca, G., Exploring Digital Government transformation in the EU -Analysis of the state of the art and review of literature, EUR29987EN, Publications Office of the European Union, Luxembourg, 2019.

6 World Bank 2016. "World Development Report 2016: Digital Dividends", Washington D.C.

- Increases inclusion as people get access to services that they could not have before, and;
- Makes government more responsive to its citizens.

Digital Government involves rethinking organizations and processes and changing behaviour so that public services are delivered more efficiently to people. Digital Government in its basic form is about automating and computerizing systems and transactions which in turn leads to increased transparency, accountability, and decreases the opportunities for gratifications[7]. A digital transformation maturity model provides a suggested journey for countries, to give context to PNG's strategy.

Digital Government is designed to promote and improve stakeholder contributions to development, as well as to deepen the governance process. It does this by increasing the quality of government service delivery, allowing for better use of government infrastructure and resources. It also provides for improved governance, empowers the private sector to partner with the government to develop Digital Government services, and increases transparency, and accountability.

1.4.2 Nature of Digital Government Services

Digital government services refer to web-based (online) and electronic forms of government services. In some cases, these are digital versions of manual, face-to-face, and/or paper-based government services. In some more effective cases, these are altogether new government services re-constructed to achieve objectives in altogether new ways.

For example, in Estonia a citizen can complete a tax return in about 3 minutes because the tax return is prepared by a digital government service and the citizen only has to confirm that they agree or not. Data from bank accounts and accounting firms and the tax department are blended electronically and the citizen save hours, if not days, preparing their annual tax return.

1.4.3 Types of Digital Government Services

The three types of digital government services are:

- Government to Citizen (G2C): These are the services that the Government provides to its citizens (consumers) using technology to streamline the delivery of services and benefits. It describes the relationship between government and consumers. G2C allows consumers to access government information and services instantly, conveniently, from everywhere, by use of multiple channels.

- Government to Business (G2B): These are the services that the Government provides to Businesses. The opportunity to conduct online transactions with the government reduces red tape and simplifies regulatory processes, therefore helping businesses to become more competitive.

- Government to Government (G2G): Governments depend on other levels of government within the state to effectively deliver services and allocate responsibilities. In promoting citizen-centric service, a single access point to government is the ultimate goal, for which cooperation among different governmental departments and agencies is necessary. G2G facilitates the sharing of databases, resources and capabilities, enhancing the efficiency and effectiveness of processes. It allows Governments to operate more efficiently and effectively, reduce costs and cut red tape. Whether it means reducing cost by reducing paper clutter, staffing costs, or communicating costs with private citizens or public government. It also allows for the collaboration of several different government systems talking to each other to exchange information, identify and authenticate users, and process transactions.

7 Gartner's model is helpful here: https://gtnr.it/2Zi6KOw.

1.5 Key Considerations

This policy makes the following key considerations which it expects will guide planning and implementation:

1.5.1 Integrated Government

Integrating government systems and infrastructures across the whole of government is a key objective under this Policy. It requires detailed consultations across all levels of government, and with businesses and the civil society.

When making integrated government considerations are being made several principles (derived from the lessons learned and experienced of other countries' digital transformation journeys and tailored to the PNG situation) are helpful.

Principle 1: The Once-Only Principle

The once-only principle (OOP) is central to joined-up government. The OOP requires that individuals and businesses should not have to supply the same information more than once to public entities. Interoperability of databases is key to realizing this principle.

Principle 2: Federation with Digital Standards

A federated approach means different departments are free to design, implement and manage whatever ICT systems they determine are required for their needs – however – this is done within the confines of a set of whole-of-government digital standards.

Whole-of-government digital standards will ensure that federation doesn't mean chaos. Equipment would be procured in common tiered configurations based on requirements. Data would be stored in a common format to maximise interoperability and exchange and independence of proprietary formats. Applications used in government for common functions like office productivity would be standardised to gradually move to a common standard of digital literacies among the civil service. Data in a department would follows a consistent set of classifiers and lifecycle for management, e.g. a document might go through the following stages: draft, review, published, confidential; and always include the date of last edit and the ID of who edited it. Rules for good computer hygiene would be implemented to minimise the potential for cyber vulnerabilities to be exploited.

A federated approach with digital standards will maximise autonomy of departments but maintain a sufficient degree of interoperability and consistency to reduce costs, remove complexity, improve cyber security, lower training costs, and improve digital skills and productivity among civil servants.

Principle 3: A Place for Everything, and Everything in Its Place

This principle works in concert with the OOP – each government department takes inventory of the data it holds and determines what it is authorised to collect and keep and what it is not. A data controller for each department takes on the job of data resource organisation and right down to the level of an individual data item in a table in a data; say a citizen's current address; is assessed and its legitimate home determined. If in the course of that process of analysis it is discovered that another department is responsible, then a data sharing agreement must be put in place so that a citizen's data only resides in the places it is permitted to reside by law or regulation. No other data is retained or asked for or collected at any time by a department.

Countries like Estonia use systems like X-Road, which combine the ID of digital, legal, and natural persons, mediated by data sharing agreements to form a network of data flows that adhere to common standards and are logged for legal and regulatory compliance and auditing purposes. The government of Estonia cites it

now saves around 16,000 person-years of work for each year they automate information flows throughout the government.

Having a secure common information exchange platform is the key to federation and to avoid the never-ending tasks of integrating the whole of government by building individual system-to-system links. After just two or three systems are interlinked, the number of system-to-system links becomes unmanageable – the number of links grow quadratically using this architecture.

But using a single common information exchange all systems across government can be linked together with a linear amount of effort, i.e. add one system and one link between that system and the common exchange and the result is total integration: see Annex C for a diagram that shows the difference between the number of system-to-system links needed in a whole-of-government digital ecosystem adopting dedicated system-to-system links and adopting a federated approach with a secure information exchange – the difference in cost, complexity, time, and resources is significant and the reason why federated models are often the only sensible choice for e-government.

1. The ability to identify digital, natural, and legal persons which send and receive digital data;
2. A standards-based digital identification scheme used to attribute data to the correct party and to encrypt that data so that only authorised parties can ever access it;
3. A neutral and tamper-proof digital service that time stamps data flows between digital, legal and natural persons, and finally, and;
4. A system of registering those data flows in a ledger to provide a secure and legally reliable audit for archiving and logging of electronic records and data exchanges.

1.5.2 Digital Identity

The identification of natural, legal, and digital "persons" is a key enabler of many other SDG goals and targets. Specifically, SDG goal 16.9 is to, "by 2030, provide legal ID for all, including birth registration".

The ability to provide reliable and independent proof of your ID is essential to modern daily life. As the world digitalises, a digital ID is the new key enabler of the growth of electronic commerce and digital government, and an engaged and empowered civil society. According to the World Bank, an estimated 1 billion people worldwide do not have the means to identify themselves—including as many as 1 in 4 children and youth whose births have never been registered—and many more have IDs that cannot be trusted because they are of poor quality and cannot be reliably and independently verified[8].

ID comes in two main types: *foundational* and *functional*. An example of a *foundational* ID is one recognised in the laws of the country and issued by a government agency like an identity card. An example of a functional ID would be what a bank issues to a customer under the terms and conditions of service and so they can transact with the bank.

In digital transactions and interactions, the quality of an ID – i.e. the degree to which it can be trusted - largely depends on the issuer of the ID. If the issuer is trusted, then the ID inherits that trustworthiness. If the issuer is not trusted, then the ID inherits the same. The issuer can be trusted if it is well governed and uses the right technologies to implement security without secrecy.

8 Online source: https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable, Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable, accessed: 19 May 2020.

Digital ID can be applied to three actors: natural persons, legal persons, and digital persons. Natural persons represent physical and distinct human beings. Legal persons refer to corporate entities and distinct legal bodies[9]. Digital persons can be thought of as the computers, applications, and devices that make up the modern global digital infrastructure. As these digital entities take on more significant roles in society, identifying them digitally is critical.

The Role of Digital Identification in e-Commerce

Being able to easily, reliably, and independently verify a person's identity is critical for economic development and in particular for e-commerce. A digital ID helps a company to trust that their customers will pay for goods and services. A digital ID equally helps customers to trust the companies they transact with. A digital ID lowers the operational costs of doing business (see Box 2 in Annex B). Transactions between customers, companies, and the payment service providers that facilitate the payments between them, can be moved online if there is a way to identify all parties.

A digital ID for legal, natural, and digital persons also improves regulatory compliance as systems for record keeping can be automated, archives for auditing can be generated without human effort, and monitoring and reporting can be assigned to a system rather than a person.

In PNG, where road infrastructure is limited, using the Internet to link up businesses and customers is vital to some kinds of e-commerce, bridging difficult geography and distance. A digital ID is the key to unlock this development potential for e-commerce.

The Role of Digital Identification in Digital Government

A digital ID will also enable government services to move online. Knowing who is on the Internet interacting with government facilitates transparency, efficiency, and effectiveness of government service delivery.

First, each digitalised "transaction" can be attributed to the unique parties involved in the transaction, whether they be legal, natural, or digital persons. Knowing the unique parties involved in a government "transaction" curbs official graft and corruption because the opportunities for human interference in the transaction is either removed or to varying degrees limited.

Second, transparency over, and permanent record of, who is involved in a "transaction" is an effective disincentive for misbehaviour and provides an automated but permanent record for compliance and the ability to later audit what took place.

Third, a trusted digital ID enables public services to be targeted precisely at the intended group of citizens. Knowing who the beneficiaries of public programs and services are means less waste of public resources and a greater positive social impact when the right people receive government support.

Fourth, and finally, a digital ID reduces the operational cost of public administration. In Nigeria, biometrically enrolling civil servants in a government payroll system saved roughly US$74m in the first year through the removal of 43,000 ghost workers. In India, digital ID held in mobile phones has reduced public education teacher absenteeism. In Argentina, using a single digital ID system allowed 13 government databases to be done away with and improved tax collection by US$104m[10].

9 Actually, the term 'legal persons' includes 'natural persons', but we use the term 'legal person' more exclusively here to refer to only corporate bodies and distinct legal entities recognised under the law in PNG and exclude human beings from this category.

10 Clark et al. 2016. "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation", World Bank Group, GSMA, Secure Identity Alliance, Discussion Paper, July 2016.

A trusted digital ID is not just about filling in biographic data forms, capturing biometric scans, and registering that information in a database. The success of a digital ID scheme is determined by the following critical factors:

- Is the digital ID scheme *trusted* and to what *degree* is it trusted?
- Who are the parties that trust the digital ID scheme?
- How easy is it to present the digital ID to a relying party?
- How long does it take to be authenticated and authorised using my digital ID?
- Is the scheme certified by an independent certifier for its governance and security protocols?
- Does the scheme disclose how it collects, stores, protects, and transmits personally identifiable information (PII)?
- Does the scheme make use of a formal consent mechanism for the data it uses?
- Is the scheme federated or centralised – in other words who can enrol citizens in the scheme?
- Does the scheme use and disclose the international standards for governance and security it adheres to?
- Is the scheme open for anyone to rely upon and use?
- Does the scheme disclose a public charter or guiding principles?
- Does the scheme allow an end user the right to be forgotten or deleted?

Digital ID in government is typically based on an open framework for trust and international standards wherever possible to maximise interoperability and maintain technology and vendor independence (i.e. to avoid being locked into a particular vendor or technology).

In PNG, open "trust frameworks" are a new concept and although only a single identity service provider (IdSP) exists at this time and promotes an open trust framework for digital ID[11], use of such a provider should be encouraged by government for a number of reasons

- A digital IdSP will contribute to broad adoption of digital services as a citizen can identity once and then be accepted at every institution that joins the ID scheme,
- A digital IdSP can easily scale because it does not require face-to-face interaction or visiting central physical locations to obtain,
- A single digital IdSP is easier to regulate than the entire economy and every institution that manages a digital identity for their customers,
- A digital IdSP prevents customers from repeatedly identifying themselves at each and every institution which is a considerable loss of productivity and resources as every institution is establishing trust between it and its customers, but that trust is not transferrable or leveraged to other institutions.
- Without transferability or leverage of the trust earned in one institution into other relationships, the customer is effectively locked in. To move away to another institution the customer has to commence the identification process all over again which is a sizable disincentive to switch. Competition is therefore limited between institutions.
- A digital ID also enables, within the rights bestowed by law and regulation, for maximum visibility over the citizen for the purposes of monitoring for misbehaviour and financial risks like credit fraud or money laundering and terrorist financing.

11 The Digital Identification Bureau Ltd. was formed in 2018 under the auspices of the BPNG and the PNG Digital Commerce Association Inc. The identification scheme is known as "YuTru" and is the first fully digital identity service provider in the country to commence issuing open standards-based and independent digital identities in 2021. YuTru is directed by its shareholders which include numerous state-owned enterprises and private companies and is observed by the BPNG.

Digital ID that is issued by a single individual institution is usually only accepted at that institution, e.g. think of a bank debit card ID. It cannot be used to assert an ID to a police officer. The true utility of a digital ID is not just to possess one for its own sake or to build trust with a single institution, but to provide access to needed services because it can be obtained once and trusted anywhere and everywhere within the economy. This is when the citizen derives the maximum benefit.

But, to be trusted, digital identification schemes must to be open and standards based, and security must not come from secrecy but instead from secure algorithms, good governance and recognised control mechanisms. Digital ID that is issued by a dedicated IdSP is independent of any one business that needs to rely on the ID. The IdSP is considered an honest broker because it only benefits commercially when it is trusted and openly accepted anywhere and everywhere.

An IdSP is the ideal way to scale an ID scheme quickly because relying parties join the scheme to benefit from the trust and independence that the scheme bestows upon its business, when the business adopts the scheme's rules for digital ID.

The digital ID scheme also needs to use privacy-enhancing techniques by default, not as an after-thought, to protect the PII of those citizens who are on the digital ID system. The use of 'privacy by design' and 'security without secrecy' principles ensure that citizens' data cannot be joined or used without consent.

For example, in Austria special cryptographic techniques are used to ensure that a citizen identifier is never stored across multiple government databases which would enable two or more departments to join citizen data from their respective database to build a profile of the citizen. Each sector receives an identifier which is unique within their sectoral data set and linked to the citizen mathematically, but which is different from the identifier provided to any other sector the citizen interacts with. Joining of data can only be done with the consent of the citizen or by law.

Digital identification in PNG must make use of this and other privacy enhancing techniques as a matter of course, and draw upon the specific expertise available internationally so that our identification systems enhance a citizen's well-being and maintains their right to privacy and the protection of their data, while they access digital government services.

By designing the digital ID system based on open and international standards, the ID system can also be more sustainable and interoperable with other government systems abroad, both in the region and internationally.

For example, currently, central banks in the Pacific region are being encouraged to participate in a regional facility to make and answer requests for knowledge of customers who make cross-border payments. Payments across our national borders must be monitored with knowledge of who the transaction parties are to manage AML/CFT and other financial risks. Digital ID simplifies how that can be done, and our government commitments in the region and internationally to combat financial crime better upheld.

There is a need to develop a comprehensive legal and regulatory framework to enshrine the recognition and protection of digital ID into law and regulation. Regulations like the BPS 253 "Customer Due Diligence" standard for authorised financial institutions have already been revised to make such provisions for full digital identification and verification of customers without requiring face-to-face interactions and without reliance on government-issued paper-based identity documents; this is a sign of the financial sector preparing for digital ID and the government should consider doing the same.

This Policy and the Digital Transformation Law represent another step. Other legal instruments will be required to enshrine: the protection of citizen privacy and their PII data in government and the private sector; the requirement for consent to use their data; citizen access to government data and information; the 'right to be forgotten'; digital signatures (as distinct from electronic signatures); communications decency; a revised ICT strategy, a revised electronic evidence Act, and an update of the PNG cyber security policy. These are just some of the rights and responsibilities that need the backing of law and regulation for digital ID to open the door to

digital government services.

1.5.3 Privacy & Trust

Privacy and trust are vital elements in digital transactions, underpinned by, among others, the key principles of confidentiality, integrity and accessibility of data. The government must be able to give assurance and prove that PII entrusted to its custody will be kept safe and secure from exposure, leakages, theft, tampering, and/or damage.

Confidentiality ensures that PII data and information will only be disclosed to the authorised parties. Integrity means that PII will be free from tampering or corruption. Availability means PII will be accessible at the right time and only to authorised parties.

Addressing privacy concerns of citizens will foster trust, as will transparency over the use of citizen PII data and information. Building trust between citizens and authorities is at the core of a functioning e-government. Considerable emphasis should be placed on communicating with citizens about how and for what reason their PII data will be collected, stored, processed, and/or shared by and within the government. Without trust, users feel vulnerable and marginalized and are reluctant to take advantage of the many legitimate benefits that e-Government offers.

User trust is important to the future success of the Internet because if users do not trust the Government, they may even cease using it for certain activities. This could have a serious impact on the use and growth of digital government.

Building user trust does not just mean reassuring people and hoping for a positive outcome. Building user trust requires the government to actively disclose what they are doing with PII and adhering to strict privacy rules and showing that they are doing so in a transparent way. Regular updates, disclosed protocols, identifying who within a government department is the controller of data, providing a mechanism for recourse when a citizen's right to privacy is breached; are just some of the trust building methods the government can put into policy and implement to create new norms around handling PII data in government.

Apart from new norms for how organisations behave with PII data, there are privacy enhancing technologies that contribute to building user trust. In section 5.2 of this report we list numerous techniques for privacy protection which need to become standard criteria for providers of government applications and systems. These are often absent from domestic applications used in government and those offered by the private sector. This must change if the applications and services are to be trusted with the PII of our citizens. The domestic market must be willing to compete and demonstrate how is has implemented privacy-by-design principles in its applications and technology services if it is to stand a chance at being competitive against foreign application and services and win government contracts.

2 STRATEGIC FRAMEWORK

Digital Government is about planning and coordinating the integration of information and communication technology in public administration through various government processes, operations, and structures with the purpose of enhancing Government to Government (G2G), Government to Consumer (G2C), and Government to Business (G2B) transparency, efficiency, accountability and citizen participation via, and vice versa.

The 'Digital Government' pillar under the 'ICT Roadmap' identifies key activities for the PNG Government to implement. Key among these issues is integration of all government systems into a single ICT platform to enable a single platform for:

- Online access to government data anytime, anywhere;
- Shared infrastructure, information and services;
- Improved productivity through digitization of civil services;
- Online e-government services promoting innovation, and;
- Centralized ICT procurement for the public sector, promoting cost effectiveness and standardisation.

2.1 Digital Government Strategy

In a future document, the GoPNG will develop a *Digital Government Strategy* to guide the development of future policies, investments, and implementation mechanisms, to ensure that digital transformation helps PNG achieve its development objectives. This strategy document will set out the "future state" that PNG aspires to be, and the means of implementation to accomplish specific goals along the way. It will focus on the actions and resources of stakeholders, including but not limited to, academics and technical community, NGOs, and the private sector, as well as the many government departments and agencies that have a role in the development of PNG's ICT-enabled development priorities.

The goals of the *Digital Government Strategy* should include:

- Enabling citizens to access high-quality digital government information and services anywhere, anytime, on any device in any of the national languages;
- Ensuring that government procures and manage devices, applications, and data in smart, secure and affordable ways, and;
- Unlocking the power of government data to spur innovation across sectors and service areas.

The vision, goals, and objectives below form the heart and centre of the following eight key ideas, specifically:

- Citizen-centred;
- Efficiency;
- Productivity;
- Infrastructure;
- Cost reduction;
- Governance;
- Improving Transparency, Accountability, and Service Delivery, and;
- Increasing Innovation & Economic Development.

Digital government helps to increase the transparency of decision-making processes by making information available and accessible to all citizens. By putting government services online, digital government reduces bureaucracy and enhances the quality of services in terms of time, content and accessibility. Efficiency is attained by streamlining internal processes, eliminating the need for customers to write the same information on each form, thereby enabling faster and more informed decision-making.

In endeavouring to achieve efficiency, the following objectives are identified:

- To provide effective leadership of National Government efforts to develop, coordinate and promote secure digital government services and processes by establishing appropriately the Department of Information and Communication Technology which will amongst other functions, establish and have direct oversight of the National Centre for Public Data and Interoperability, the National Cybersecurity Centre, Communications Command and Control Centre, National Public ICT Infrastructure Authority;
- To promote the use of the Internet and other information and communication technologies to provide increased opportunities for citizen participation in Government;
- To promote inter-agency collaboration in providing digital government services, where this collaboration would improve the service to citizens by integrating related functions, and in the use of internal digital Government processes, where this collaboration would improve the efficiency and effectiveness of the processes;
- To promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services;
- To reduce costs and burdens for businesses and other Government entities;
- To promote better informed decision making by policy makers;
- To promote access to high quality Government information and services across multiple channels;
- To make the National, Provincial, and Local Level Governments (LLG) more transparent and accountable;
- To transform agency operations by using, where appropriate, best digital service practices, and;
- To provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws.

A key component in the implementation is having Ministries and Agencies understand their roles and responsibilities. This is imperative if the implementation and sustainability of newly initiated government systems, platforms and other initiatives are to be successful. Ministry Officials need to have an awareness that digital government services and processes extend beyond the mere automation of existing procedures and that the current procedures may not necessarily be efficient or effective.

To drive this transformation, the strategy is built upon several overarching principles.

An **"Information-Centric" approach**—Moves the government from managing paper or electronic "documents" to managing discrete pieces of open data and content which can be shared, secured, and presented in the way that is most useful for the consumer of that information on timely basis.

A **"Shared Platform" approach**—Helps the government work together, both within and across agencies, to reduce costs, streamline development, apply consistent standards/guidelines, and ensure consistency in how the government creates and delivers information and promotes governance.

A **"Customer-Centric" approach**—By this we mean, how the government Influences how data is created, managed, and presented through websites, mobile applications, raw data sets, and other modes of delivery, and allows customers to shape, share and consume information, whenever and however they want it.

A platform of **"Security and Privacy"**— This platform will ensure that innovation happens in a way that ensures the safe and secure delivery and use of digital services to protect information and privacy.

For the executive and legislative arms of government, digital transformation enables a structured foundation for its digital ecosystem. Transformation within the public sector cuts across all levels of government. In response to a global and national shift towards a digital economy, governments are on a path to embracing virtual meetings, online documents, services and processes, thereby drawing from other global government successes and failures, best practices, standards and guidelines.

For the general business sector, this would include:

- Leveraging ICT to improve the business environment;
- Connecting small enterprises to larger ones and the global marketplace;
- Delivering financial and business development services; speed up the development of skills in citizens to meet this challenge, and;
- Enhancing the competitiveness and innovative capacities of small businesses.

For the education sector it means:

- revamping the entire educational system to integrate ICT into all aspects of the curricula and making sure the students are digitally literate as well as physically literate;
- promoting e-learning, and;
- protecting children online.

For the health sector, this includes:

- integration of existing isolated health and life event databases;
- securing and enabling trusted and authorised real time access to vital citizens' health information and records bearing personal and clinical data; and
- enabling remote access to specialist consultation and information over and above the limits imposed by physical distance vis-à-vis telemedicine.

For the finance, trade and economic sectors, ICT integration will lead to:

- access to financial and banking services;
- promotion of a Whole-of-Government secured data and information exchange point for relevant agencies and organisations to partner to enable ease of doing business and trade; and
- promoting anti-money laundering (AML) and counter terrorism (CT)-related activities.

For the agriculture sector, ICT integration will include:

- development of agricultural databases and digital services;
- enhancing rural-based employment and entrepreneurship as well as rural urban connectivity in poor, under-served rural and coastal areas;
- promoting ease-of-access to instant updates of market information, instant access weather conditions and instant dissemination channel for training and essential information for farmers; and
- support greater collaboration and opportunity for logistics services to ease movement of farm produce to market places.

For the social and law enforcement and security sectors, integration:

- improves implementation capability and productivity of relevant agencies; and
- supports the development of national and institutional law enforcement and security capabilities.

For academia and civil services organisations, integration grants:

- access to public official government information and services; and
- promotes the ability for academia and civil services organisations to participate in government policy formulation, implementation and monitoring and evaluation.

2.2 Challenges

2.2.1 Open Retail Market

The GoPNG will work hard to ensure that there is no excessive concentration of market power by one or two operators since this concentration leads to monopolies and inhibits future innovation.

2.2.2 Digital Literacy and skills

Digital literacy and skills is critical to make effective use of access to data and technologies and also to gain employment in a new digital world. The networked society requires new expertise: digital and technological literacy, communication skills, problem solving, critical thinking, self-learning, teamwork, change management, creativity, and initiative. Understanding this interplay at a relatively detailed level is critical to leveraging this technology for educational reforms.

Education systems must shift from textbook knowledge to teaching how to learn and become agile problem solvers. Much of this learning must occur through networks that cut across academic, business, local, and global communities.

Developing quality, updated and relevant digital skills across universities and educational institutions and across all sectors has been a major challenge. Industry and private learning institutions are leading the way with digital literacy and skills compared to the public sector. Digital transformation seeks increased collaboration and partnership with industry and private learning institutions through establishment of innovation hubs, and centres of excellence.

2.2.3 Remuneration

Employing and maintaining a service of highly trained and experienced professionals within the current public service framework, but at salaries which are benchmarked to the private sector is the key to digital transformation. These professionals are providing the technical expertise to implement new business models, change processes, information technology, systems and operations. Shortages of IT staff and voluntary turnover jeopardize digital transformation projects and create a competitive disadvantage to the government in its effort to attract highly qualified professionals to remain within the public sector.

3 POLICY OBJECTIVES

3.1 Vision

Our vision is digital transformation that makes government closer to the people through effective governance, improves service delivery, and fosters inclusive social and economic development enabling a smart, networked, and well-informed society,
that:

- Promotes collaboration, interaction, and participation;
- Promotes innovation and learning;
- Provides an open and transparent government, and;
- Provides citizen-centred services, and knowledge-based industries.

3.2 Mission

To bring about our vision we will do the following things:

- Increase the quality of government service delivery;
- Improve productivity and efficiency of the public service;
- Demonstrate better use of government ICT infrastructure and ICT resources;
- Improve internal governance and processes of government;
- Reduce costs;
- Promote innovation and entrepreneurship;
- Empower the private sector to supply e-government services government partnership;
- Increase transparency in public administration through digitalisation, and;
- Develop the right digital skills and enhance digital literacy.

3.3 Goals & Strategic Objectives

We recognise how we have achieved our mission by the following overarching goals and strategic objectives:

- Goal 1: To establish and improve a nationally coordinated management and promotion of secure electronic government services, particularly G2G, G2C, and G2B through federation with standardisation principles and to enable and trigger the structured establishment and consequently promulgate PNG's digital economy.
- Goal 2: To build national infrastructure, including software and applications ecosystem required to facilitate digital government and other relevant ICT facilitated service delivery for the benefit of the citizens.

3.3.1 Sub-Goal 1: To develop models, programs and projects for digital government.

Strategic objectives:

a) Develop sustainable models for development and funding of digital government;
b) Develop digital government programs and projects that impact on the lives of PNG citizenry;
c) Build capacity and skills within government for productivity and efficiency;
d) Align government programs and projects with digital government, and;
e) Develop national skills to build and operate the required information systems.

3.3.2 Sub-Goal 2: To develop benchmarks, standards, guidelines and framework of interoperability for digital government applications, systems, processes and organizations.

Strategic objectives:

a) Ensure that all applications deployed by government agencies are interoperable for seamless data exchange and integrity;
b) Provide standards and guidelines for ICT use and applications in government;
c) Guide government in the use and applications of ICT within itself;
d) Provide benchmarks for projects and programs for effectiveness;
e) Partner with the Industry and domestic and international organisations to provide technical leadership for standards and technological infrastructure, and;
f) Promote free enterprise and open source standards.

3.3.3 Sub-Goal 3: To develop, operate and maintain a national e-government system which will enable seamless data collection, integration, shared services, and authentication.

Strategic objectives:

a) Provide a one-stop online gateway for 24/7 access to government services;
b) Provide a national platform for common shared services amongst government agencies;
c) Ensure that all Government forms are online for easy access;
d) Ensure that data collected by government agencies are protected with strong encryption;
e) Provide national standards for government agencies' websites and social media pages;
f) Ensure that government agencies are able to share and reuse resources for efficiency and productivity to reduce cost and avoid waste:
g) Promote Innovation and entrepreneurship; and
h) Encourage private sector participation in delivery of government services.

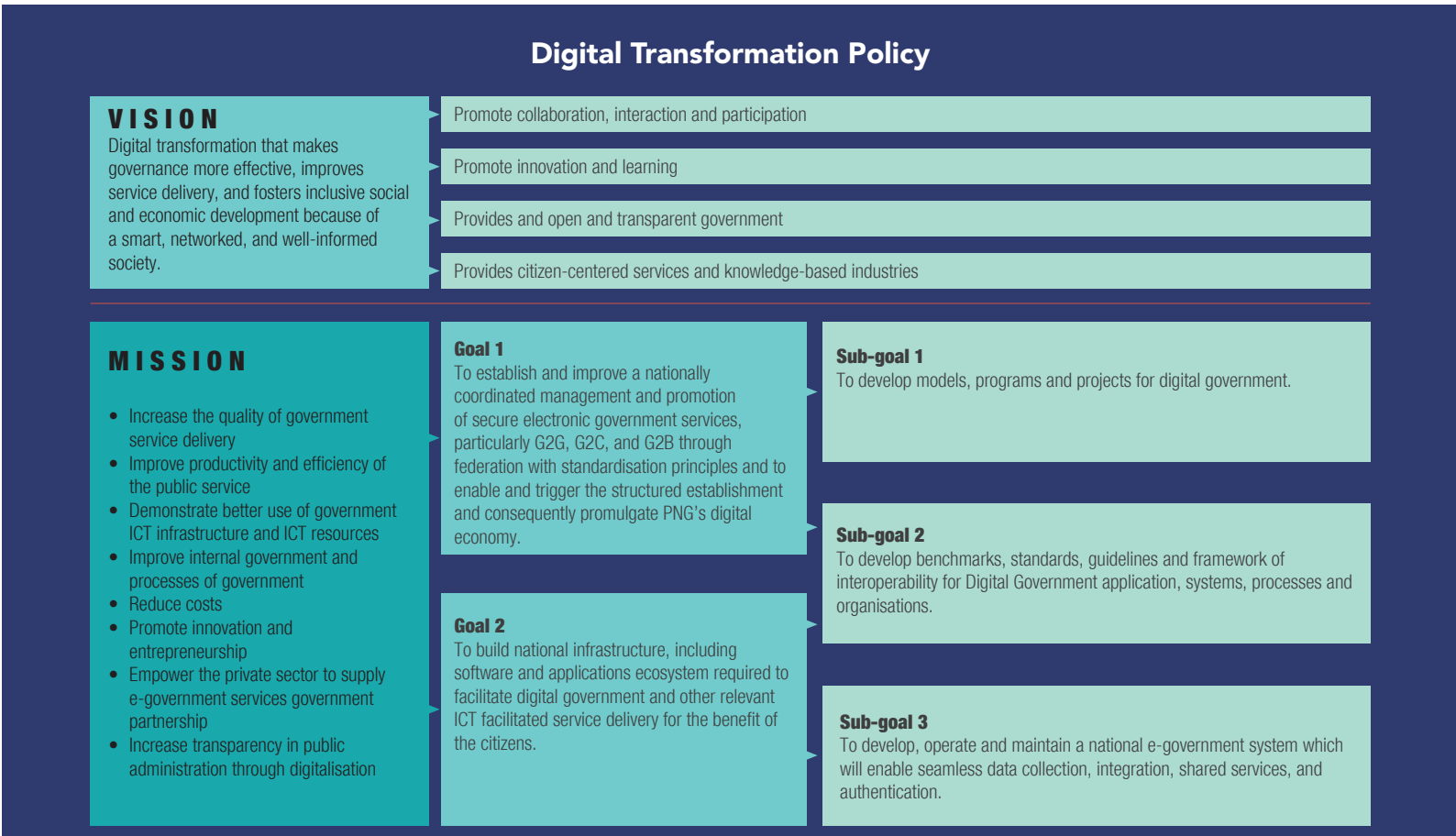


Figure 1 Structure of the PNG Digital Transformation Policy

4 POLICY SCOPE

The scope of this Policy is broad in nature and generally reflective of the framework set out in the ICT Roadmap (2018). This document builds on six thematic areas in which the government departments and agencies will work, together with the Ministerial Committee on ICT (MCICT), and with input from the technical community, the private sector, academics, and civil society to integrate government systems from national to provincial and district into a single GoPNG computing environment.

This Policy covers six thematic areas: (1) digital infrastructure; (2) digital government; (3) digital skills, (4) innovation and entrepreneurship, (5), cyber-safety and privacy, and (6) financial inclusion. The relationship between this Policy and how it will be implemented in the DICT and across government is depicted in Annex D.

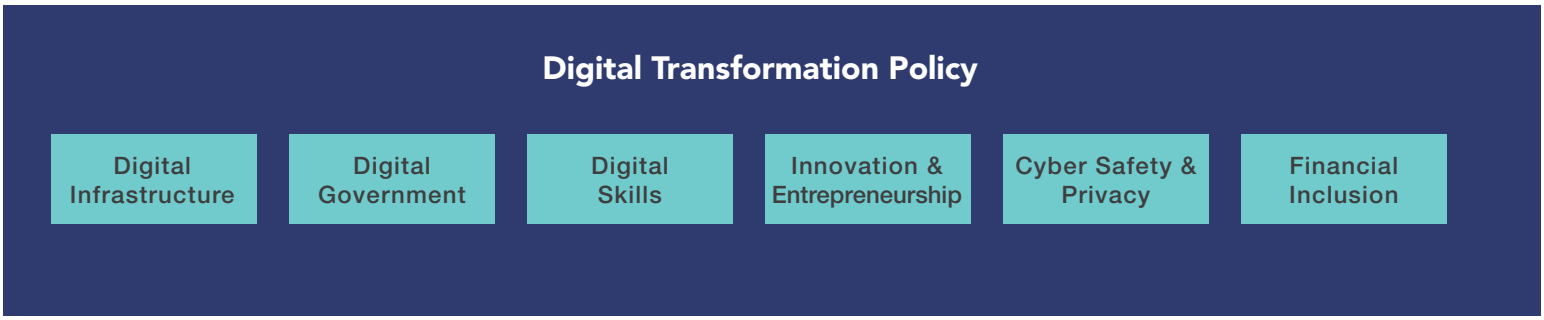


Figure 2 The six thematic areas of the PNG Digital Transformation Policy

4.1 Digital Infrastructure

Digital infrastructure underpins the delivery of digital services. Rolling out widespread, modern and resilient infrastructure with sufficient capacity is key to development of the ICT sector in PNG. Activities within this framework area are focused on developing the universal availability and high quality of broadband telecoms networks, and supporting infrastructure such as data centres, internet exchange points (IXPs), international gateways and payment platforms.

Initiatives within this area should also aim to ensure that infrastructure is deployed in a way that encourages either effective competition and/or supports the provision of affordable services. The GoPNG has previously invested in a private Government Network. However, this program has not gained traction to full expectation. To that end, it is helpful to note how other jurisdictions have developed their infrastructure regulation to varying degrees.

4.1.1 Infrastructure Sharing

There are different models for how network operators can share network infrastructure, but they generally fall into two main categories: *passive infrastructure sharing* and *active infrastructure sharing* (GSMA).

At the most basic level, *passive infrastructure sharing*, the physical infrastructure such as land sites, conduits for utilities along roads, towers, site power, and backhaul assets are regulated for equitable sharing to any network operator once it is constructed.

Active infrastructure sharing goes one step further permitting service providers to access the core network, radio transceivers, and even the spectrum itself using various methods for multiplexing and frequency hopping to allow more than one network operators' data to be carried across the same electromagnetic spectrum.

Infrastructure sharing regulation ensures that all network operators and service providers have equitable access to the same "on ramps" to PNG's electromagnetic spectrum, regardless of who constructed the "on ramp". Infrastructure sharing regulation incentivises new network operators and/or new service providers to utilise existing network components rather than build their own.

This improves competition because the capital required and the time to construct the network are significant barriers to entry for a new network operator or service provider. It also, naturally, reduces overall quantity of physical infrastructure that has to be developed in the country, as network components are largely only built once and then shared among subsequent entrants.

At present in PNG, each network operator, in large part, has had to and continues to build their own infrastructure.

Not only is this a blight on the natural landscape of the country, but it duplicates costly infrastructure and introduces years of delay in expanding the network and disincentivises competition.

An inability to share the infrastructure among telecommunications carriers creates a number of market distortions which prevent wholesale and retail prices for telecommunications services from falling. The high wholesale costs are passed onto the retail customer.

4.1.2 Wholesale & Retail Competition in Telecommunications Services

Excessive concentration of market power by one or two companies leads to monopolies and inhibits future innovation. When combined with digital components, digital technologies can strengthen these other components and accelerate the pace of development. At present, PNG's wholesale market comprises two carriers:

(i) a state-owned wholesale network operator investing in terrestrial and submarine network infrastructure, and (ii) a private network operator, an incumbent with large investments in the same.

Without a policy and regulation for mandatory sharing of telecommunications infrastructure, there is little incentive for the incumbent to share its physical infrastructure and permit new entrants to the wholesale or retail markets and thus compete. New entrants are effectively blocked from developing and offering new telecommunications services because they cannot afford to erect their own infrastructure.

If incumbents cite that physical infrastructure, they have invested in, is incapable of being shared, then the infrastructure will need to be phased out or brought up to a standard that permits it and all future infrastructure plans to cater for sharing. NICTA will need to set those physical and logical infrastructure standards. Poor or limited access should be no excuse for preventing access altogether.

The state-owned operator cannot reduce its wholesale prices to an internationally comparable price for two interlinked reasons. First, to attract the other retail service providers to buy capacity on the wholesale network, and at a lower price than the incumbent internally pays for that infrastructure they have invested in. It must be superior service as a retailer is not going to switch for lower prices if the service reliability and quality affects the retail products they offer. Second, in order for the state-owned operator to be able to lower its prices, it requires both wholesale volume and operational efficiency to reach whole pricing levels that make it a profitable business. Neither of these conditions are in place today and have been the subject of debate for many years. This Policy promotes looking at international best practice for the regulation of utilities to learn how best to serve the PNG market.

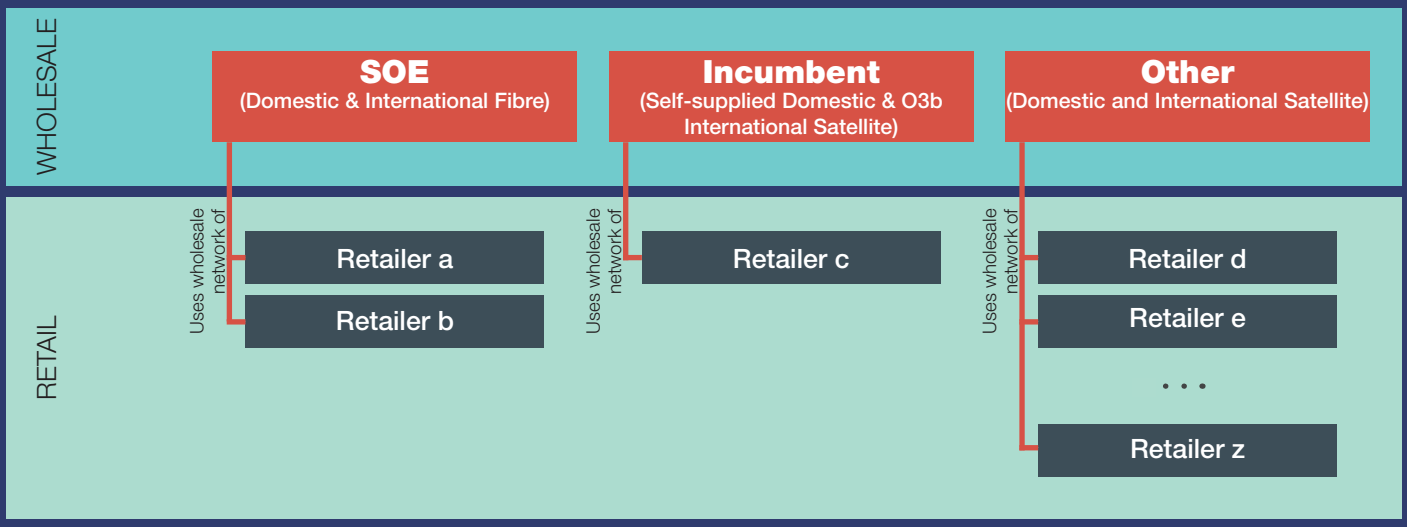


Figure 3 Structure of the PNG wholesale and retail telecommunication market.

Some observers have made nuanced and specific recommendations to reduce prices and lift quality in the telecommunications sector: harmonise the costing models used for wholesale price determination, implement effective infrastructure mutualisation policy to force sharing of the "on ramps" to access the natural resource that is PNG's electromagnetic spectrum, joint public and private ownership of the national wholesale network operator, a well-functioning UAF that gradually increases in size over time, among other things.

For the new investment made in the Coral Sea Cable to realise gains for the economy, wholesale competition must be sought and the current siloed operations of each wholesale network operator (i.e. the state-owned operator and the incumbent) must be broken down if margins are to be maintained, retail price reductions forthcoming, and telecommunications and data service quality are to improve.

Internet connectivity affects the core aspects of governance. With good quality low-cost connectivity comes an increase in the government's capacity to deliver services more conveniently, at lower cost, and to all citizens. Lower transaction costs, leads to greater inclusion, overcoming information barriers, enhanced efficiency, and streamlining and automating transactions. They also support efforts to increase government accountability, through citizen empowerment to communicate.

4.1.3 Universal Access Fund

Another tool used by countries to expand Internet infrastructure and lower cost for new entrants to the market to foster competition, is the universal access fund (UAF). Use of a UAF must be nuanced and deliberate, though, because there are some strict and well-tested limits to be learned from other countries so the UAF contributes effectively to expanding access.

The most controversial of parameters is the size of the UAF levy applied to service providers. International comparison of UAFs show that no more than 2% of the revenue in the sector is ever disbursed in a single year, no matter how effective or the size of the sector. In fact, the amount is usually much lower, between 0.3% and 1.1% of gross revenue in the sector.

Also important is the basis of the levy calculation - i.e. top line revenue, specific telecommunications products, with and without exemptions, etc. – which determines what degree carriers, operators, and providers could potentially "game" the accounting used to calculate the basis of the levied contribution to the fund

In some countries, use of a dedicated and experienced external fund manager, rather than administration by a government department, provides independence and can improve transparency. The fund manager is

given a set of performance measurements and incentives aligned with the UAF's objectives the fund manager incentivised based on the impact or effectiveness of the UAF.

If carriers, operators, and providers can see the UAF monies made available in a timely and regular fashion, and applications for funds are determined in a transparent, fair, and orderly process, then the UAF can become a powerful incentive for market participants to extend physical infrastructure into less profitable market segments and geographies.

Finally, it is important to also recognise the difference between definitions of "universal access" from "universal service". Service objectives and measures are less meaningful without a sufficient degree of access across the country for citizens. PNG is challenged from the latter at this time, making plans of universal service unwarranted at this time, and potentially counterproductive to efficient operation of a levy-based fund.

4.1.4 Private Government Network

DICT surveyed public sector IT expenditure and found that the GoPNG currently spends K160m annually for general telecommunications and Internet services with private Internet Service Providers (ISP). This expense is broken down as follows: K40m for Internet access, K100m for telephony services, and K20m for dedicated Internet connections, data storage and website hosting. In comparison, it would only cost GoPNG K40m annually, once the switch to the IGIS and shared services was made – a material saving of K100m each year.

In 2005, the GoPNG expressed its desire to create a private government network – the Integrated Government Information System (IGIS) - where government departments would be interconnected. Consequentially, *NEC Decision No. 124/2006* endorsed the proposal to integrate government agencies through a common information platform and directed the DICT to implement the recommended steps set out in the *E-Readiness and Feasibility Study* to that end.

The original IGIS policy was aimed at harnessing the latest IT to computerise and integrated government departments and agencies to create more efficiency and administration quality in the public sector. It was envisaged that e-governance would promote a responsive, efficient, and responsible government with the objective of enhancing national development. In the original vision the National ID Project was under the purview of DICT but later on it was moved to the Ministry of National Planning.

In 2009, a *Cost Benefit Analysis Study* was commissioned to evaluate the IGIS concept. The study's findings showed that the project was economically viable and would provide both cost savings and an improvement in government service delivery. The IGIS project was endorsed by Cabinet (under NEC Decision, 50/2010) and the DICT was directed to implement the project.

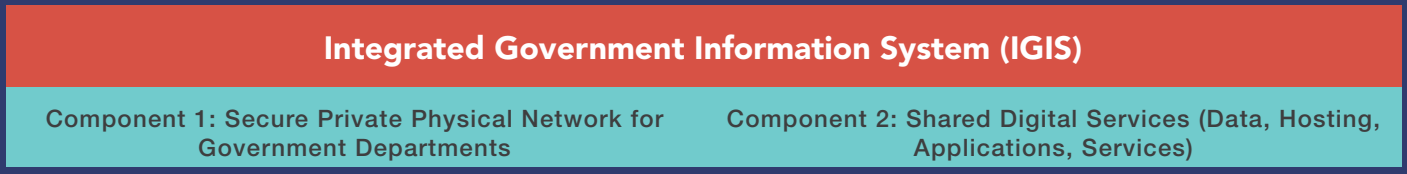


Figure 4 IGIS components include a network and shared services.

The second component of the IGIS project was to establish a secure private high-speed government network, within the NCD, to link government agencies to the new data centre and its shared services and applications. The aging communications network was first upgraded to a 10 GB "ring" metropolitan area network (MAN), with funding under the IGIS program. The fibre network now consists of 12 cores equally shared between IGIS and PNG Telikom and enables connection between the data centre and 47 agencies' sites. Outside the NCD, the network was extended to six provincial agencies.

The goal of the IGIS network rollout phase 2 and phase 3 projects were to extend connectivity and basic communication services from the NCD to various subnational agencies. However, IGIS phase 2 and phase 3 were never executed.

A government private network has been considered ideal for the GoPNG but will be subject to major capital investments. Besides connectivity, IGIS would encourage other departments to place their data in the new data centre to create economies of scale, improve security, and reduce external data storage costs. It would more importantly spur the procurement of goods and services at scale for the whole-of-government and enable negotiation of better prices for increased volume.

4.2 Digital Government

This pillar is composed of both the infrastructure needed to transform the sector and also the applications and services that will be deployed on the digital government architecture. This includes digital ID and digital payments.

Digital government requires a better understanding of how technology interacts with other critical success factors to PNG's successful digital transformation. The use of different ways of computing - other than the current on-premises client-server model – has resulted in savings to government computing costs of 80% or more. Cloud-based applications allow a pay-to-use model of computing which avoids the sunk cost of expensive upfront and renewal software licenses. Thin-client and virtualised computing has been shown to create savings as high as 86% of the total cost of ownership[12] when compared to client-server computing, as is used across the 122,000-computer environment of the GoPNG.

If these well-established technologies are used in developed country governments like Australia, Singapore, and New Zealand to reduce the cost of government computing and to use taxpayer funds more efficiently, how much more important must this consideration to look at alternative computing models be for the GoPNG given our resource constraints?

Thin-client and virtualised computing have the potential to remove the need for uninterruptible power supplies (UPS) and their maintenance. Also, a thin-client is unusable without the accompanying thin-client server making them a poor target for theft. A thin-client computer also can last as long as 8-12 years, a lifecycle 200-300% of a typical desktop or laptop PC.

The digitisation of services can bring significant cost savings for governments, and the infrastructure deployed to support e-government can promote wider access to digital services. Digital infrastructure, enterprise architecture, and services or applications delivered through them enable government to respond directly to the needs and demands of citizens. They also ensure that citizens have the same experience whether they access government information on their PC, mobile, or tablet devices or in -person.

Short-term activities within this framework focus on digitising high-volume transactions (such as tax payments

12 Willenberg 2018, "Government Computing Models: Handbook with Implementation Guidelines", Neocapita Security Consulting, 26 June 2018

or birth registrations) to promote the use of ICT for citizen-to-government interactions and building awareness and take-up of ICT. Digital payments will allow citizens to pay for these services using their mobile phone.

Digital government systems help all stakeholders overcome information barriers that are impeding service delivery, but if these systems are not implemented correctly, governments remain unaccountable. Moreover, the empowerment and inclusion gains expected may not come and the result could be government systems that are less accountable.

Delivering government services digitally can drive take-up and use of digital services, both inside government and across the wider PNG public. Digital Government systems help all stakeholders overcome information barriers that impede service delivery, but if these systems are not implemented correctly, the government will remain unaccountable. Moreover, the empowerment and inclusion gains expected may not come and the result could be government systems that are less accountable

Digital infrastructure is important in enabling connectivity, but it is the adoption of online services that use this connectivity which will create value for PNG. Citizens and businesses can benefit from access to information, tools to improve productivity and efficiency, and improved access to services such as health and education. These include all digital government services such as ability to pay taxes, vote, pay utility bills, school fees, register for school, conduct business online, access education and health records.

Activities within this framework are focused on promoting the provision and take-up of affordable, relevant digital government services, communication of digital government services, and supporting the development of local digital content.

4.3 Digital Skills

Digital government systems automate many tasks but if workers do not have the necessary skills for these jobs, the efficiency gains may not materialize and instead there could be greater inequality. This pillar is so integral to the adoption of digital government, digital transformation, and the growth of the PNG economy that it will be integrated into all the pillars of digital transformation.

More than two-thirds of all jobs in PNG are susceptible to automation, which means that there will be far less low-skilled jobs and many more middle to high-skilled jobs available in this new economy. This may not result in large-scale unemployment. But it will lead to a greater widening of the inequality gap.

Because PNG citizens need the necessary skills to use digital services, promoting digital literacy among citizens and businesses will be a key component of developing a strong ICT ecosystem. Providing practical ICT skills training to targeted segments of the population can increase demand for digital services and grow the digital economy.

Access to “first order” skills and theory to create a digital economy are hard to acquire organically in PNG; if we look at cases like South Korea and India, which cultivated enormous technology sectors by setting up the right enabling environment for technology transfer and upskilling to take place from abroad. For example, South Korean telecommunications engineers who worked within the state-owned carrier were part of a decade long exchange program with the US and in particular some of the leading telecommunications engineering firms there like Qualcomm. South Korean engineers spent time abroad at the expense of the South Korean government but under conditions of employment bonding, so they would be contracted to return and repay the investment made by their government to send them abroad. They would then return and repay the investment by teaching, coaching, and mentoring other engineers back in South Korea for years upon their return.

The same dynamic of technology transfer took place between Indian software engineers who staffed dozens of high-tech Silicon Valley start-up and enterprises, only to return to India and deploy their newly acquired software skills to solve homegrown problems. This was largely a function of the US H-1B visa type and the "Dot Com" crash which set the conditions for the Indian software development workforce to return home.

Even "second order" digital literacy skills – those are the skills acquired by using complex software systems developed by others – are difficult to organically acquire as the information and skills are not available for free. Either, (a) it costs money to acquire the skills and knowledge through proprietary vendor training and certification or (b) it requires purchase of the system in order for staff to be trained and even "see" the system and how it is designed. If the software is not purchased, access to see it, understand its design, and learn how to use it is locked behind a company's intellectual property protections.

To bring in the requisite skills from abroad in both first and second order technology skills, a concerted policy shift must be considered so that the source of that training can be acquired without paying out government funds to foreign countries, when there are lower costs and more effective ways to access the information and knowledge using existing development assistance mechanisms the government already has at its disposal and on favourable financial terms.

The Government will create training programs to provide the education needed by the current workforce, and digital skills and literacy will also be taught within departments, agencies, and universities. Partnerships will be necessary with civil society, technical and academic organizations to help the Government design and develop a human resource development portal for essential digital skills and services.

In the longer term, the development of an ICT curriculum for educational institutions ranging from K-12 and computer science at the tertiary level, will help to create a skilled ICT workforce and thus support the development of a vibrant local ICT sector.

4.4 Innovation and Entrepreneurship

Innovation and Entrepreneurship are integral to digital transformation. We need to find new and innovative ways for enhancing and expanding ways to do business in PNG.

Digital Government is about empowering and motivating everyone from civil servants, academia, technical community, NGOs, and the private sector to collaborate on different projects. For example, by opening up government data sets it allows the private sector to then take this data and create new applications and new innovations.

Technology enables governments to create positive business climates by simplifying relationships with businesses and reducing the administrative steps needed to comply with regulatory obligations.

We need to incentivize and encourage people to engage in major change and innovation both within Government and outside the government.

For public sector employees, we need to empower and motivate them by encouraging everyone to make suggestions about changes or improvements to processes, systems, or programs. We need to create a clear sense of mission, delegate authority and responsibility to all workers to enable them to solve their own problems and come up with creative solutions to these problems.

Innovation in digital government is also about empowering the private sector to start creating digital government services and applications that can reduce transaction costs and provide significant savings in performance and in money; by enticing the private sector to partner with the government to develop e-Government services, thereby increasing transparency, and accountability. GoPNG will strive to create Digital Innovation Ecosystem

to help young entrepreneurs focus on solving the local problems while learning from global solutions.

Digital Transformation includes connecting small enterprises to larger ones and the global marketplace. It means delivering financial and business development services. It means enhancing the competitiveness and innovative capacities of small businesses so that they can create new apps and continue to grow the economy. Small businesses are the lifeblood of every economy. The more we can help them the more they can create more innovative digital services to grow the economy.

Government can work closely with both public and private sector, the technical sector and civil society to ensure that PNG welcomes and rewards Innovation and Entrepreneurship. GoPNG can assist the establishment of an innovative business environment by supporting technology and innovation hubs, crowdsourcing, challenge programs and revising policies on taxation, financial support and business incubation. The adoption of appropriate digital technologies by businesses should be encouraged, along with support for the growth of start-ups and micro, small and medium enterprises (MSMEs) in priority sectors.

ICT and digital government platforms can contribute to job creation, improve the provision of social services, facilitate research, and induce other services that can raise the living standard of people. Essentially, creating the right environment can accelerate the creation of an information society where every member and every place in the society are connected.

4.5 Cyber Safety & Privacy

The take-up of digital services can be promoted by providing a safe, secure digital environment. A key step in developing a thriving ICT ecosystem is to provide PNG consumers and businesses with the confidence they need to undertake transactions online. It is here where the DICT will work closely with all agencies to assist them in improving their cyber hygiene, increase their awareness of cyber threats, and provide resources to help agencies ensure that critical infrastructure and services are protected. DICT will work closely within the basic and higher and technical education sector to increase awareness of digital safety, cyber awareness, data privacy and data protection.

4.5.1 Cyber Security & Trust

Tools to prevent fraud and promote trust should be developed and provided to consumers and businesses. Mutual trust is the key to interactions in which the government collects information about citizens and citizens provide their own data to the government. Without trust, users feel vulnerable and marginalized and are reluctant to take advantage of the many legitimate benefits that the Internet offers.

Trust is a key ingredient for a sustainable, evolving and global Internet. It is the cornerstone for all successful connectivity strategies. An 'open and trusted Internet' is a globally interoperable Internet that cultivates innovation and creates opportunities for all. Its foundation lies in user trust, technologies for trust, trusted networks and trustworthy ecosystems.

Building user trust means putting in place the right infrastructure (trusted networks), empowering users to protect their activities (technologies for trust), setting the right policies, and providing a responsive environment that properly addresses users' well-founded concerns (trustworthy ecosystem).

Equally important is ensuring the cyber security of all critical ICT infrastructure in PNG and preventing cyber-attacks. This will help to create a stable environment and promote the use of digital services

4.5.2 Data Protection

While security is necessary for protecting data, it is not sufficient for addressing privacy. Ensuring the confidentiality of data provided by individuals and organisations is extremely important and essential in ensuring that all have confidence and trust in the Government's handling of their confidential and personal data. The government will do more than develop data privacy principles to ensure the protection of the data the government is collecting. Data protection policies and legislation, which will derive from this Policy, are separate policies and legislation that will ensure citizen data is protected. The government will enact data protection policies and legislation to complement this Policy and the ensuing legislation.

4.6 Financial Inclusion

Financial inclusion is defined as the availability and equality of opportunities to access financial and digital government services. It refers to a process by which all individuals including people of any gender, race, religion, or ability and all businesses gain access to appropriate, affordable, and timely financial products and services which include digital banking, loans, bill paying, and insurance products.

Financial inclusion means that all individuals and all businesses have access to useful and affordable financial products and services that meet their needs – transactions, payments, savings, credit and insurance – delivered in a responsible and sustainable way. However, close to a third of adults – 1.7 billion – are still unbanked, according to the latest Findex data[13].

About half of unbanked people include women in poor households in rural areas or out of the workforce. The goal of financial inclusion is to remove barriers, both supply side and demand side and allow all people access to finance. Supply side barriers are those which stem from financial institutions themselves and often indicate poor financial infrastructure and include lack of nearby financial institutions, high costs to opening accounts, or documentation requirements.

Financial inclusion has been identified as an enabler for 7 of the 17 Sustainable Development Goals. According to the World Bank, when countries take a strategic approach and develop national financial inclusion strategies and institute a national financial inclusion strategy, they increase the pace and impact of reforms.

Being able to have access to a transaction account is a first step toward broader financial inclusion since a transaction account allows people to store money and send and receive payments.

The United Nations defined the goals of financial inclusion as follows:

- Access at a reasonable cost for all households to a full range of financial services, including savings or deposit services, payment and transfer services, credit and insurance.
- Sound and safe institutions governed by clear regulation and industry performance standards.
- Financial and institutional sustainability, to ensure continuity and certainty of investment.
- Competition to ensure choice and affordability for clients.

13 The Global Findex database is the world's most comprehensive data set on how adults save, borrow, make payments, and manage risk. The 2017 edition includes updated indicators on access to and use of formal and informal financial services. And it adds new data on the use of financial technology (fintech), including the use of mobile phones and the internet to conduct financial transactions.

5 STANDARDS, GUIDELINES, AND METRICS

Standards allow technology from different departments and environment to work with each other, for data to be exchanged easily, and to establish trust so that digital environment can operate predictably and with less human intervention.

Using digital standards:

- Provides a common "language" to measure and evaluate performance;
- Enables interoperability of digital equipment, application components, and data flows, even if they are from different sources and vendors;
- Adopt relevant international and national standards, and;
- Protects consumers by ensuring safety, durability, and quality.

Standards and guidelines provide a common "language" that allows staff at all levels within an organization, whether it be a government department, a private business, a university, or an NGO—and at all points in a supply chain—to develop a shared understanding of concepts and designs and implementations. Risks, mitigation, resourcing, the project lifecycle; are other things that can all be set out in common terms to improve how information is disseminated and improves understanding.

Digital government services developed by departments must adopt a set of core principles committing:

- To the use of open international, de facto and de jure industry, and non-proprietary standards;
- To preserve a citizen's right to privacy, to be asked for consent, and to be forgotten, and;
- To adopt an accessibility and human-centred design ethos.

5.1 Open Standards

Open standards can also promote and prioritise the use of open source, open data, and interoperability. Open standards also contribute to protecting the government from being held to ransom by a vendor because of being locked into the vendor's product.

5.2 Privacy

Privacy protecting techniques are numerous and each contribute in a certain way to protecting Public Identifiable Information (PII). Handling PII is often overlooked in government system and service designs, but we expect these to become norms in products and services of digital government.

Methods like encryption, obfuscation, tokenisation, sharing/distribution, zero-knowledge proofs, explicit consent, audit trails, and meta data logs, are just a small number of the privacy enhancing techniques incorporated into modern digital government systems and services. For PNG, these must become the norm or part of minimum service standards when handling citizen PII.

5.3 Accessibility

Accessibility is one of the most important aspects of modern web development. Accessibility means the greatest number of users can view your content. It means search engines will be able to read your site more completely. Users of all types will have a better experience if you take accessibility concerns into account.

Human-centred design focuses on the end user, creating a seamless, simplified and unified digital interface and experience. This will be discussed later in the section on website strategy.

5.4 National Accessibility Standards and Guidelines

Government may adopt international web standards that define what is needed for accessibility, which includes standards for websites, tools, and technologies designed and developed that allow people with disabilities to use them to enhance the ability to:

- Perceive, understand, navigate, and interact with the Web, and;
- Contribute to the Web.

Web accessibility encompasses all disabilities that affect access to the Web, including auditory, cognitive, neurological, physical, speech, and visual.

Web accessibility depends on several components working together, including web technologies, web browsers and other "user agents", authoring tools, and websites. The W3C Web Accessibility Initiative (WAI) develops technical specifications, guidelines, techniques, and supporting resources that describe accessibility solutions. These are considered international standards for web accessibility; for example, WCAG 2.0 is also ISO standard ISO/IEC 40500.

The Web Content Accessibility Guidelines (WCAG) are part of a series of web accessibility guidelines published by the Web Accessibility Initiative (WAI) of the World Wide Web Consortium (W3C). The W3C is the main international standards organization for the Internet. They have created a set of recommendations for making web content more accessible for people with disabilities—but also for all user agents, including highly limited devices, such as mobile phones. WCAG, is a set of guidelines making digital content accessible for all users, specifically, users with disabilities.

The WCAG standard:

- outlines best practices for making web content universally perceivable, operable, understandable, and robust;
- defines criteria for successful inclusive web design, with ascending levels of compliance;[14]
- Is composed and reviewed by a global community of digital experts; and
- Connects the world through common information technology and user experience standards.

5.5 National Digital Services Standards and Metrics

A strong internal digital governance structure will help public agencies develop coherent priorities, set up lines of accountability, and satisfy the public's expectation of the best possible level of service. Public agencies must manage their websites and digital services; not as discrete individual IT projects, but as part of a comprehensive strategy covering all their digital information and services. To manage this:

- Every agency must establish a plan for governing its digital services, including websites and data, and;
- Ensure compliance consistent with best practice in the following areas:
  - Use Analytics and User Feedback to manage websites and digital services. All public facing websites and digital services should be designed around user needs with data-driven analysis influencing management and development decisions. Public agencies should use qualitative and quantitative data to determine user goals, needs, and behaviours, and continually test websites and digital services to ensure that user needs are addressed;
  - Public agencies' public websites must contain a search function that allows users to easily search content intended for public use;
  - Agencies must ensure that all content intended for public use on their website can be indexed and searched by commonly used commercial search engines;

14 WCAG 2.0 and 2.1 outline three levels of compliance. Level A is the highest priority and usually the easiest to achieve. Level AA is more comprehensive. Level AAA is the strictest, most comprehensive accessible design.

- Public agencies must disseminate information to the public, structured in a way that enables the data to be fully discoverable and usable. Open and publicly accessible data can increase public participation in government, promote transparency and accountability, and increase government operations' efficiency and effectiveness;
- Public agencies must be transparent about policies and practices with respect to Public Identifiable Information (PII), and must provide clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII;
- All public agencies must post Privacy Policies on their websites;
- All public agencies must implement Information Security and Privacy Controls. Information technology changes rapidly and agencies must have the flexibility to address known and emerging threats while making continuous improvements;
- Use Secure Connections (HTTPS). The public expects Federal Government websites to be secure and their interactions with those websites to be private. Unencrypted HTTP connections create a privacy vulnerability and can expose potentially sensitive information that is susceptible to interception, manipulation, and impersonation. This data can include browser identity, website content, search terms, and other user-submitted information;
- Use Only Approved Domains with a gov.pg domain. Along with gov.pg email addresses. E.g. Do not use a Yahoo, Hotmail, or Gmail address; The administrator of the .PG domain will establish SLA for the issuance of .gov.pg domains so that the process will be quick and convenient for public agencies and MPs to obtain;
- Ensure Information Quality and Accuracy. Information disseminated from Government websites and digital services, or from third-party services on behalf of the Government, is expected to be authoritative and reliable;
- Use Plain Writing Web content as it is most effective when it is easy to understand, find, and use;
- Ensure a Consistent Look and Feel Across Websites;
- Centralize and streamline procurement and usage of ICT products and services for all public and statutory bodies;
- Compel and facilitate the in-country hosting and centralization of all government data and information, and sharing of data and information between government to government, government to citizen, government to business and vice versa; this will be done through:
    - development and implementation of central and open data policy, and;
    - development and compliance of interoperability standards;
- Facilitate and compel cyber security standards and compliance for all public and statutory bodies;
- Facilitate and coordinate digital government services specifically: government to government, government to citizen, government to business and vice versa, to increase public service delivery efficiency and reduce government expenditure. For example, e-Voting, e-Census, e-Tax, e-Agriculture, e-Police, e-Education, e-Parliament and range of e-services;
- Facilitate and coordinate digital information dissemination and communications and data sharing for government to government, government to citizen, government to business and government to employees and vice versa;
- Facilitate growth of the digital economy through development and implementation of other relevant policy, programs, and projects pertaining to digital skills, digital services, and digital infrastructure; and
- Public Agencies are to comply with any ICT Procurement Policy defined by DICT with respect to the hosting of a website.

5.6 Website Design and National Digital Content Strategy

The GoPNG will publish a web design and national digital content strategy document that every public agency that is using a Government domain will be required to follow. At a minimum, this strategy will also include the type of content needs to be listed on each government-owned website. For example, the strategy will include:

- Design and layout of the web page;
- What links are required and the purpose they serve;

- The text that you should use for each link;
- Where the link should be located on your site, and;
- Which law or policy requires those links;
- Descriptions of the mission and statutory authority of the agency;
- Information about the organizational structure of the agency; and
- Government information and services that should be readily available to the public regardless of device.

Agencies must, to the extent practicable, ensure that their public websites and digital services perform equally well on non-desktop devices such as mobile devices and tablets.

On a primary agency site, one should include information about the agency with descriptions of the public agency organization structure, mission, and statutory authority, and links to the following information:

- The agency's strategic plan and annual performance plans;
- The agency's privacy policy page;
- The agency's point of contact;
- The agency's Open Government page; and
- The agency's Plain Writing page.

Secondary agency sites also need an "About" page that describes your site and links to your own website policies. It should also include links to the primary agency's "About" page.

5.7 Social Media Guidelines for Government

Social media is a powerful communication channel. It can be used to reach target audiences with strategic, effective and user-centric interventions. In a separate document, DICT will outline protocols for the coordination, standardization and streamlining of government information dissemination on social media platforms. DICT will do this by drawing up a series of guidelines to assist agencies in the planning, development and implementation of social media activities. These guidelines will provide critical information on lessons learned, best practices, clearance information and security requirements for information to be put up on national and provincial websites and for agencies to use social media to reach their customers. It will also establish guidelines for naming and ensuring compliance for all Government social media pages. For example, Agencies that do not adhere to these guidelines may be forced to take down their social media until they comply with the guidelines.

Social media tools such as Facebook, Twitter, and text messaging allow agencies to expand their reach, foster engagement, and increase access to credible messages. Social media can also help organizations achieve their goals some of which are to:

- Disseminate information in a timelier manner;
- Increase the potential impact of important messages;
- Leverage networks of people to make information sharing easier;
- Create different messages to reach diverse audiences;
- Personalize messages and target them to a particular audience;
- Engage with the public; and
- Empower people to make safer and healthier decisions.

When integrated into communication campaigns and activities, social media can encourage participation, conversation, and community. This is extremely useful in helping to spread key messages, influence key decision makers, and promote behavioural change. Social media also helps to reach people when, where, and how it is convenient for them, which improves the availability of content and might influence satisfaction and trust in the messages delivered.

Cybersecurity is crucial for the success of any website strategy. As such, DICT will also develop a series of guidelines for the use of social media technologies and third-party software and websites by Ministries and Departments. This strategy will be enforced and sites that are not in compliance will be taken down.

All agency websites must be kept up to date both technologically (cyber-wise) and with current and correct information. This is particularly true when using these websites or other agency resources in social media campaigns. Ministries and Agencies need to ensure that their sites can defend against rapidly evolving social media threats. This can be done using a multi-layered approach, assessing risks to the individual, risks to the department or agency, and risks to the national infrastructure.

Social media technologies such as Wikis, Blogs, and social networks are vulnerable to the following methods/ techniques of cyber-attacks: Spear-phishing, Social Engineering, and Web Application Attack.

Social media presents a particular challenge for communicators because the users do not focus on a single document. People often sift through lots of information, or skim topics to determine where to focus their attention. That is why it is critical to Know Your Targeted Audience. In that way, messages can be developed that are specific to the concerns, needs, and desires of a particular demographic. Understanding what is important to your audience will increase the effectiveness of your social media efforts. Likewise, understanding your audience will help you select the best channels for reaching specific audiences with your messages.

However, just like all strategies and all communications tools, social media goals need to be reviewed annually to see if they still are effective in reaching your desired audience.

6.1 Institutional Framework

The existence of a cohesive and well-functioning institutional framework is essential for achieving the objectives of this Policy. The aim of an institutional framework is to ensure that the various institutions within the digital transformation initiative effectively play their respective and interdependent roles.

The Government will provide leadership and direction in the implementation of this Policy and this will require additional laws to be enacted.

The DICT will write subordinate policies, standards, and guidelines to assist branches of government to create the enabling environment for digital transformation in their respective departments.

Where there is a need to harmonise how a digital transformation is approached, let's say in the case of the procurement of a common and standardised set of computers by an individual government department, then the DICT will necessarily intercede at pre-agreed and vital points in the department's annual work cycle: at planning, at budgeting, and at annual review, say.

Intervention will be required to ensure consistency and harmonisation of planning approaches that include digital transformation considerations in each plan made and finalised. It is to ensure that resources are not acquired for technology that is out of step with both standards and guidelines set by the DICT. Finally, to make sure that the digital transformation has realised benefits to the citizens served by a department and the department itself, digital transformation measurements need to be taken each year when department performance is reviewed.

The relationship between this Policy and how it will be implemented in the DICT and across government is depicted in Annex D.

6.2 Role of Government

The Government's role in digital transformation will include:

- Development, implementation and coordination of policy;
- Introducing digital transformation regulations and licensing;
- Development an enterprise architecture for digital government;
- Providing a central Government ICT procurement policy; and
- Provision of an enabling environment for investment in the ICT sector.

6.2.1 Department of Communication and Information Technology

The Department of Communication and Information Technology was established in 2003 pursuant to NEC Decision No. 292/2003 dated 17 December 2003. It continues to be the policy advisory arm of the Government on all matters pertaining to the ICT sector.

In addition, the Department may consider, as part of implementing this Policy, taking on relevant project and program implementation roles. Considering the wider roles of digital transformation, renaming the Department will become inevitable. A suggestion would be for renaming the Department as "Department of Digital Transformation" or simply 'Department of Information and Communications Technology'. Other than

through enabling legislation, the ability to rename, establish, or abolish a Department of the Public Service in PNG is made pursuant to the Public Services (Management) Act 2014.

The Ministerial Committee on ICT (MCICT), for which DICT is secretariat, is currently mandated to provide high-level coordination of digital government activities across the various government departments and agencies with the aim to integrate government systems from national to provincial and district onto a single GoPNG ICT infrastructure platform. By integrating all our systems, information can be shared across whole-of-government to achieve informed decisions, and public developmental information will be made available and accessible to citizens when and where required thus empowering our citizens to be self-reliant. This is a step towards implementing the 2030 Agenda for Sustainable Development, specifically Goals 2, 3, 4, 6, 7, 8, 9, 10, 11, and 16.

The following is the current structure of the ICT Roadmap for achieving digital government:

- The Minister of ICT chairs the Ministerial Committee on ICT Issues. This committee will also receive, consider and decide on recommendations, plans and proposals from the National ICT Sector Coordinating Committee;
- The National ICT Sector Coordinating Committee shall be chaired by the Secretary, Department of Communication and Information Technology. The purpose of this committee is to:
  - Serve as a central point for assessment and recommendation of all ICT investment projects as a prerequisite to the PIP approval process;
  - Ensure integration and interoperability of all Government systems;
  - Develop a *Strategic Action Plan* for the MCICT geared towards achieving the outlined objectives of the MCICT;
  - Set the agenda and creating an action plan, on a yearly basis consistent with the National Social and Economic Development Plans;
  - Facilitate the implementation of the Strategic Action Plan; and
  - Identify any policy gaps and recommend to the MCICT for development and implementation.

The MCICT has the clear authority to broaden and restructure and reorganize the structure of the digital government roadmap as and when deemed necessary and to better suit the industry and the Government's effort at creating a digital government. The MCICT will work with other Government stakeholders and also the input from the technical community, the private sector, academic, and civil society.

Considering the current efforts to factor this overarching Policy into legislation, consideration may be made to widen the functions of the restructured Department to take on technical mandates of the Ministerial Committee.

6.2.2 ICT Sector Regulator

The National ICT Authority of PNG (NICTA), established by the *National Information and Communication Technology Act* 2009, is the regulatory body for the ICT sector particularly within the telecommunication space. A review of the ICT Policy (2008) and therefore reform of the National Information and Communication Technology Act 2009 is overdue. Digital Transformation Policy has implications and NICTA has the opportunity now to step back and assess.

6.2.3 Independent Consumer & Competition Commission (ICCC)

The Independent Consumer & Competition Commission (ICCC) is the principal economic regulator for competition, mergers and acquisitions, and price and consumer rights. Its primary role is to administer and implement the Independent Consumer and Competition Commission Act 2002 and other related legislation.

The ICCC performs a number of functions including administration of price regulation, licensing, industry regulation and other matters outlined under the principal legislation or any other act or regulation that prescribes powers and functions.

The ICCC is an independent statutory authority established in January 2003 following the enactment of the enabling act by the Parliament in March 2002. The ICCC is responsible for promoting and safeguarding competition, protecting consumer's interests and regulating declared industries, entities and goods and services.

The primary objective of the ICCC is to enhance the welfare of consumers in PNG, promote industry conduct and standards, and protect consumers interests with regards to the price, quality and reliability of goods and services.

6.2.4 ICT Appeals Panel

Certain decisions of NICTA may be reviewed by the ICT Appeals Panel established under the National Information and Communication Technology Act 2009 pursuant to Part XIII Division 2 and sections 255 to 263.

The ICT Appeals Panel is constituted from members of the panel of experts appointed under Section 41 of the Independent Consumer and Competition Commission Act 2002.

The review provides a rehearing of a decision of NICTA through a streamlined process which precludes introduction of new evidence and requires decisions to be handed down within a prescribed time period. No actions may be taken in Court from a decision of NICTA until the ICT Appeals Panel process is first exhausted. Therefore, judicial review is only available after a person has first exhausted all other remedies provided under the enabling legislation.

6.3 Role of Development Partners

Development partners will play a complementary role towards assisting GoPNG to realise the goals and objectives of this digital transformation policy. GoPNG will continue to work with its development partners to foster linkages and continue to provide financial, material, technical assistance as well as build capacity for sustainability.

6.4 Role of External Stakeholders

The role of the civil society, the technical community, and the private sector will be to inform the policy making process through relevant contributions in an effort to improve and enhance accountability and transparency of government.

6.5 ICT Professional Bodies and Start-ups

The Government will recognise and encourage the formation of national ICT professional bodies and start-ups registered under the laws of PNG to foster professional ethics, standards and human resource development.

6.6 Implementation Process

The following steps will be critical to ensuring implementation of this Policy:

1. Establishing a Digital Government (Services and Infrastructure) Act 2020 and enforcement of the legislation and related policies;
2. Restructuring DICT to ensure appropriate structure is established;
3. Developing and launching a comprehensive Digital Government Strategy and eGovernment Technical Blueprint (including the Enterprise Architecture) to implement a National e-Government Platform;
4. Developing and having endorsed relevant standards and guidelines; and
5. Establishing additional enabling legislation, such as Data Protection, Data Privacy, Interoperability, Cyber Security, Electronic Evidence, Communications Decency, Right to Information.

7 MONITORING & EVALUATION

There is global recognition that effective public sector governance requires the use of ICT to achieve more efficiency in the functioning of government and to improve the delivery of government services to organizations and individuals.

To monitor and compare the status of digital government, there needs to be a set of feasible, relevant and internationally comparable indicators. Such indicators are useful inputs to the formulation of policies and strategies for effective digital government.

Digital government enhances social and economic development by enabling improved access to government services. Examples range from better access to information on available services to complete online processing of requests for permits, certificates, payments etc. Effective use of digital government also improves the efficiency and effectiveness of the public sector and linkages between government agencies.

For the assessment of digital government, individual indicators and composite indices have been developed by international organisations, academic establishments and individual countries. The scope of interest includes single countries, regions and global measurement. Some studies assess use of ICT alone; others measure customer services through services offered via government websites.

The latter range from simple services to more sophisticated issues of privacy and electronic voting. Methodologies range from country-level surveys of
government organisations to highly complex web-based surveys.

As a policy tool, digital government indicators reflect status and trends and guide policy-making towards more efficient administration, improved services and more equal participation for citizens. Collection of egovernment statistical information faces several challenges. They include statistical feasibility, data collection costs and burden on respondents.

For any metrics, indicators, or other performance metrics that will be proposed, there are often different government agencies and different strategies that are used, which is why it is imperative for a national strategy to be issued. Whatever the data collection methods employed; digital government indicators should be:

- Statistically feasible;
- Designed to enable international comparability;
- Substantively relevant;
- Consistent, thereby enabling reliable evidence of change over time;
- Understandable and accessible to policy makers and other data users; and
- Not so complex as to limit their collection and use.

Longer-term challenges in digital government measurement relate to the relevance criterion and should reflect changing policies and technologies. They raise questions, such as:

- How should indicators evolve given technological change?
- What type of policy and strategy issues should be addressed through the indicator set?
- What is the broader impact assessment framework for e-government?
- How can digital government indicators be further elaborated?

The alignment of long-term development objectives of e-government measurement with technological change and societal needs is essential for strengthening the relevance of indicators and digital government measures.

The OECD, through its Working Party on Indicators for the Information Society (WPIIS), has been developing

standards covering a number of aspects of information society measurement since the late 1990s, including development of concepts and model surveys. Eurostat has also been very active in this field for the last decade or so, through its annual community surveys on ICT usage. The Eurostat and OECD model surveys on ICT use include questions on the use of digital government services (by individuals and businesses). The UN E-Government Knowledgebase Reports[15], the UN Partnership on Measuring ICT for Development and ITU ICT Statistics also plays an important role. Despite the range of measuring tools, the overall goal is:

- Improve the measurement of investments in ICT and its link to macroeconomic performance;
- Define and measure skills needed for the digital economy;
- Develop metrics to monitor issues of security, privacy, and consumer protection;
- Promote the measurement of ICT for social goals and the impact of the digital economy on the society;
- Invest in comprehensive, high-quality data infrastructure for measuring impacts, and;
- Build a statistical quality framework suited to exploiting the Internet as a data source.

Measuring of ICT for Development and of digital government relies on standards for government statistical units. In this vein, national standards or guidelines need to be developed for many ICT or digital government uses. Other internationally agreed standards for government surveys can be found in the Frascati Manual for Measurement of Research and Experimental Development (R&D). These existing standards for measuring characteristics of government focus on volume measures, such as expenditure, revenue and R&D staff. Stakeholders are identified as:

- Data producers, including all government agencies that collect official statistics;
- Policymakers, especially ministries and regulatory authorities dealing with ICT and telecommunications, and other data users (including international organizations), and;
- Data providers.

The coordination of data collection at the national level is extremely important. For this reason, the *PNG Strategy for the Development of Statistics* 2018-2027 together with the PNG National Statistical Office, which is established by the Statistical Services Act 1980, will be responsible for this coordination.

The development and creation of coordination mechanisms between relevant institutions, including the National Institute of Standards and Industrial Technology (NISIT)[16] , NICTA, DICT, and other ministries is key. Data providers are integral to the statistical system. Without their cooperation, data would be inadequate in terms of either, or both, quality and quantity.

Data producers must recognize the contribution of providers and prove they can be trusted as custodian. This is also one of the reasons that DICT will be authoring a new Data Privacy and Data Protection Law to ensure the confidentiality of data provided by individual organizations. It is very important that protection of such statistical data is assured and is communicated to respondents.

NISIT's role and authority in developing standards for PNG is clear and as such they should be the agency consulted when developing these measurement standards and/or guidelines. NISIT's role is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

15 https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

16 The National Institute of Standards and Industrial Technology of PNG is the government statutory national standards body established under the National Institute of Standards and Industrial Technology Act 1993. Its functions cover technical standards, metrology, conformity assessment schemes, productivity and technical barriers to trade in PNG.

Annex A OECD Digital Government Principles[17]

- Openness, transparency and inclusiveness
- Engagement and participation in policymaking and policy making and service delivery
- Creation of a data-driven culture in the public sector
- Protecting privacy and ensuring security
- Leadership and political commitment
- Coherent use of digital technology across policy areas
- Effective organisation and governance frameworks to coordinate
- Strengthen international cooperation with governments
- Development of clear business cases
- Reinforce ICT project management capabilities
- Procurement of digital technologies
- Legal and regulatory framework

17 Online source: https://www.oecd.org/governance/digital-government/toolkit/12principles/, accessed: 12 May 2020.

Box 1: Conducting a Roadside License Check in a Privacy Enhanced Environment

An example is provided here to illustrate how privacy enhancing methods can be used, without diminishing the capability of the government to perform its duties with the citizen. Think of the situation where a driver's license is checked by a roadside police officer.

In the current context a police officer might ask a driver to produce their driver's license. Doing so exposes PII of the citizen in the process of helping the police officer determine if the driver is allowed to be operating the vehicle they are driving and whether or not they have any outstanding legal matters to resolve. Let's say in this example, the driver's license shows the license number, date of expiry, the citizen's name, current home address, date of birth, and a headshot photograph.

In a privacy enhanced context, zero-knowledge proofs would be used for the police officer to make the same determinations but without revealing any PII about the driver. In the privacy enhanced context, the police officer may take a headshot photograph of the person and scan their driver's license which only exposes a machine-readable zone (MRZ), say a QR code, and nothing else. A privacy enhanced driver's license would not reveal any of the previously described attributes.

Once scanned, the mobile terminal would send the machine readable data to a system that would not return the PII of the citizen, but instead would simply answer the questions the police officer is permitted to ask and the citizen has consented to answer when they signed up for a driver's license.

In this example, the mobile terminal may respond with a "YES", to say that the holder of the license photographed matches the photograph in the system. The mobile terminal would tell the officer that "3C" is the class of vehicle the driver is permitted to operate. Given that the class was returned, the police officer would know to imply that the license is current and that to be current they must be over 18. Finally, the mobile terminal display may illuminate in GREEN to imply there are no connected outstanding warrants for this driver and the driver is free to travel on.

Box 2: How Digital Identity Can Lead to Economic Development

For example, if a company is to deliver goods or services prior to payment to a new customer, it is likely that the company will want to establish, with a reasonable degree of assurance, the identity of the customer, so the company has legal recourse and a way of collecting in the case the customer fails to pay.

Without a reliable and independent digital ID, the company usually has little choice but to expect cash on delivery or to limit the transaction value, to limit exposure and risk posed by any one customer or transaction. Also, the transaction cannot move online and is limited by geography, physical presentation of cash payments, the insecurity of the same, and human resources to process the transaction.

With a digital ID, the company can move the transaction online without limiting any recourse they have if the customer does not pay. Oftentimes, the company can accept digital payments because the customer can use the digital ID to identify themselves to their financial institution to make the payment on their behalf right from their bank account.

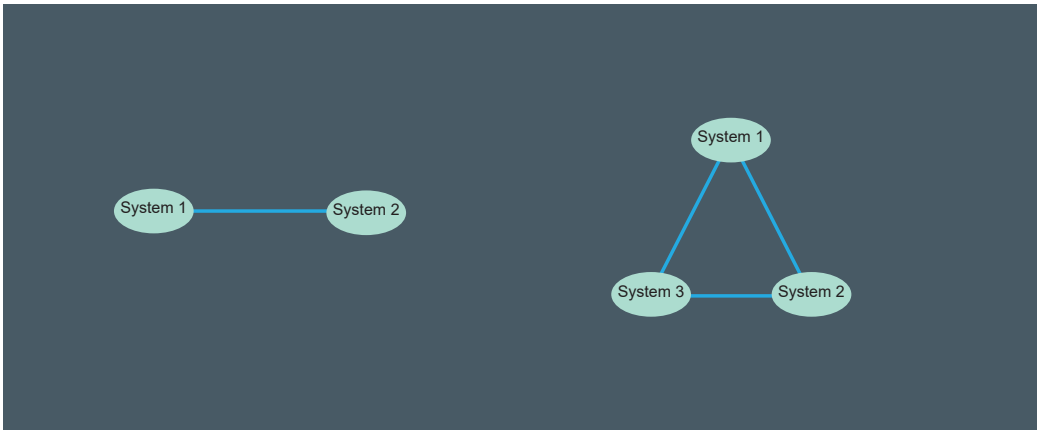
The company can then process more transactions, with fewer human resources, and much less risk that goods and services will be delivered without payment to follow.

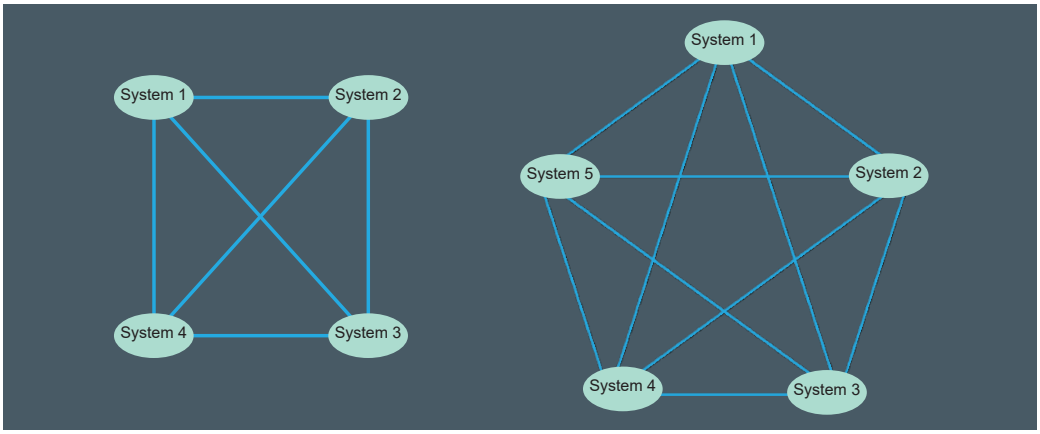
If Government adopts a system-to-system approach...

For every system the government adds making sure it is interconnected to all other systems means, the number of system integrations (i) is equal to the total number of systems (n) squared: $i=n^2$

Each system must be connected to each and every other system to achieve a fully connected government.

# Systems (n)	# Links (i)
2	1
3	3
4	6
5	10
6	15
7	21





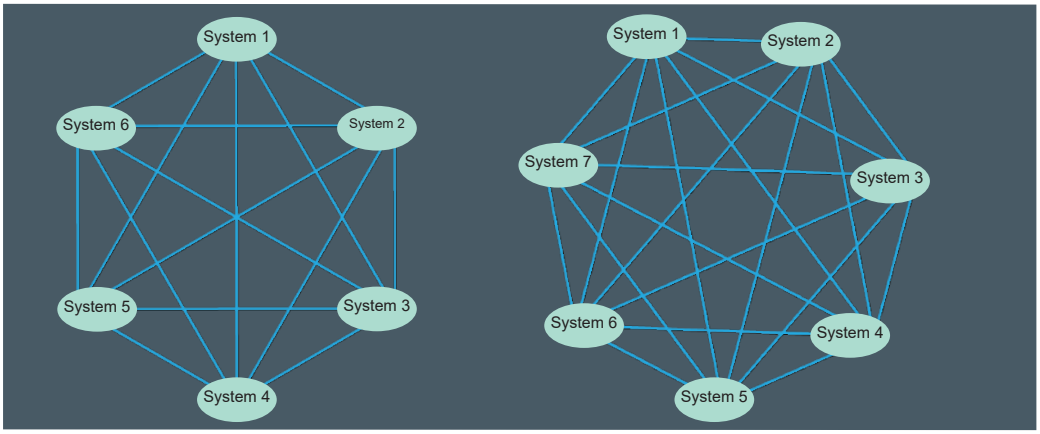


Figure 5 Using system-to-system links to facilitate integrated government information systems.

If Government adopts a federated approach with a secure information exchange...

For every system the government adds making sure it is interconnected to all other systems means, the number of system integrations (i) is equal to the total number of systems (n): $i=n$

Each system need only be connected to the secure information exchange. The information exchange acts as a sort of distribution centre for messages exchanged between systems, time stamping and logging the exchange as it occurs.

# Systems (n)	# Links (i)
2	2
3	3
4	4
5	5
6	6
7	7

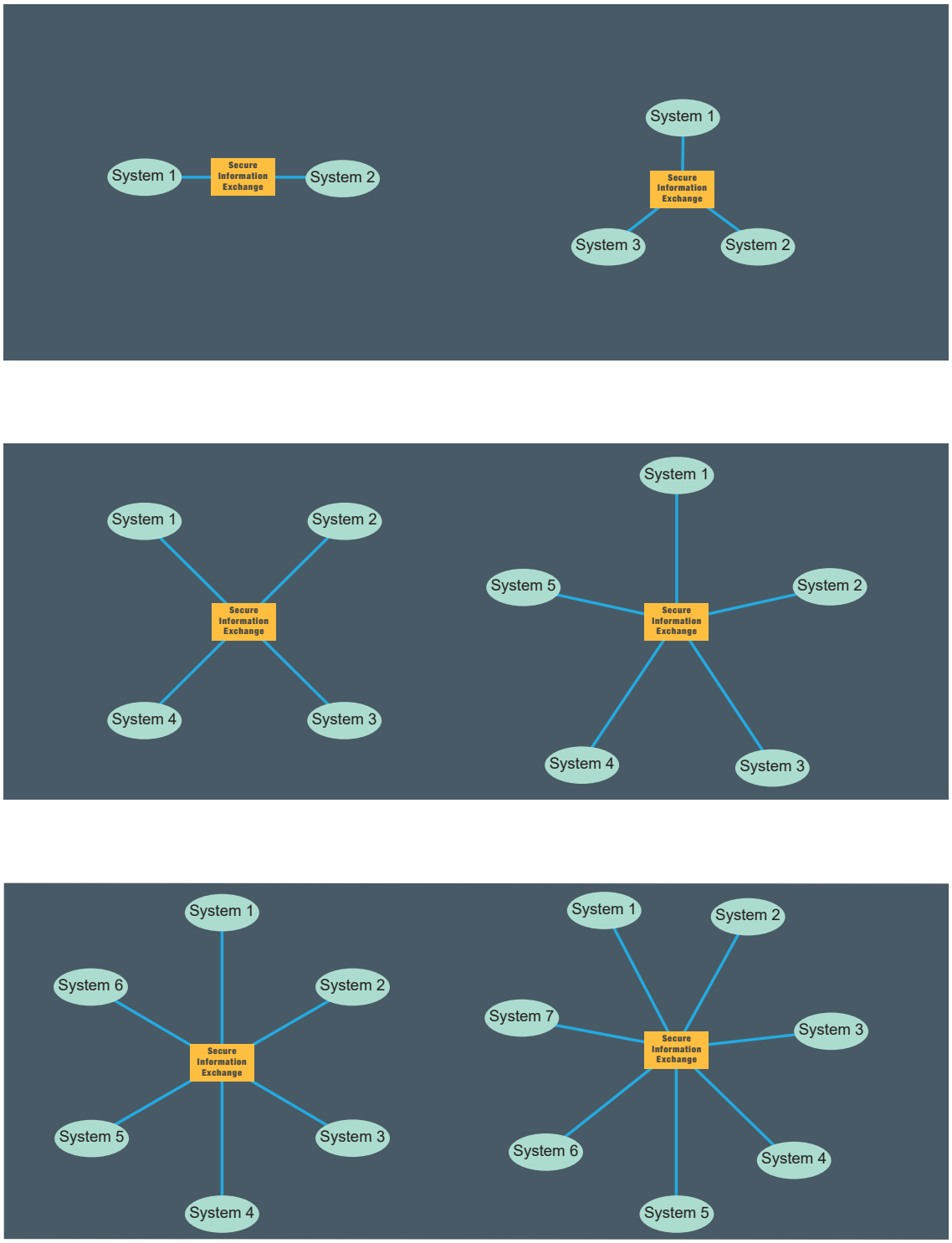


Figure 6 Using a secure information exchange to facilitate integration.

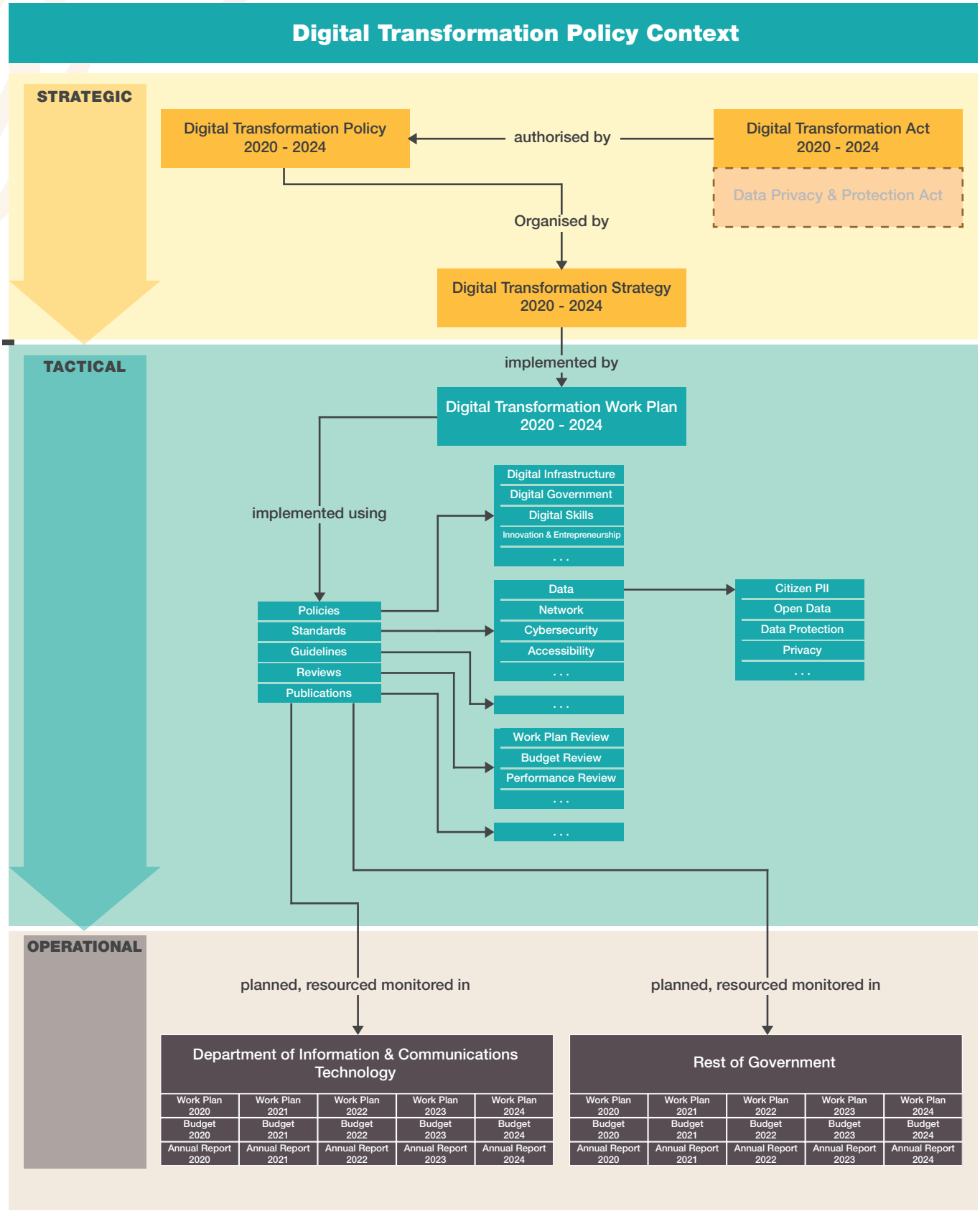


Figure 7 The digital transformation policy context