KIRIBATI

2021 Digital Government Master Plan

Table of Contents

Executive summary

Governments should ensure the best possible use of digital technologies for the benefit of the people. Digital technologies allow people to work remotely and more efficiently, communicate easily and cheaply over long distances, as well as eliminate labour-intensive jobs and time-consuming paper processes. Introducing digital technologies into the work processes of government creates transparency, enhances democracy and helps fighting corruption, while providing better and faster access to government services. A more efficient society is the main political aim of every country.

The Government of Kiribati is committed to transforming the delivery of public services and using digital solutions to enhance good governance. This is well in line with national policies, the Government Manifesto and the 20-year vision for Kiribati, KV20. The Government Manifesto declares about the improvement of the Management Information System: work will be undertaken to improve the collection, the production, the storing and release of data and news using the latest technology that is safe and efficient.

A National ICT policy was approved in 2011, which sets out the vision and the roadmap for developing a robust, stable, market-driven ICT sector. The 2019 update of the National ICT policy was approved by Cabinet in June 2019.

The aim of the current digital governance masterplan is to assess the existing digital government ecosystem in Kiribati, propose a conceptual model of an integrated digital government and compare the current situation with the model to find gaps and provide suggestions for further activities based on international practical experience. The masterplan provides an overview of the strategic building blocks of digital society – e.g. infrastructure, secure data exchange, electronic identification of citizens and businesses, population management, etc. – along with suggestions for the organisational, financial and legal framework of digital government. Also, it includes several proposals for sectorial interventions

It is efficient to have a set of reusable digital government components, which all government systems can use. Such components can not only save money, but also increase service quality. The recommendation for public administration institutions is to render access to public services independent of any specific technology or product. Therefore, the conceptual digital government model described does not predefine any architectural or technical approach.

Kiribati is currently in the process of setting up a coordination and implementation organisation, Digital Transformation Office, to lead the digital government transformation process. The implementation of digital government should be a comprehensive process, in which organisational and regulatory issues are addressed in addition to technological. There is a need for support from top political leadership and for high-level coordination, while the availability and readiness of Kiribati's public officials and technical experts can also be seen as a key prerequisite for the fulfilment of the proposed Master Plan and Implementation Plan.

A costed action plan for the next four years sets out a range of possible initial actions with timeframes and resource needs for implementation. Whereas some of the proposed solutions would be ready for immediate piloting, the implementation plan also proposes more time-consuming and ambitious goals, such as setting up the infrastructure for Kiribati's e-ID and trust services and developing national cyber security capacities.

Finally, the document also provides principles and recommendations for regulating the field of digital government, for dividing tasks and responsibilities related to digital government development, for managing the planning and implementation of the national IT budget, and setting up a communication strategy for the fulfilment of the implementation plan. The total financial estimation of the Implementation Plan exceeds 18 M AUD spread over four years. As this is a significant investment, it needs involvement of all stakeholders (including international donors). The impact and value of the digital transformation should be clearly communicated and accepted.

All recommendations presented in this report are important but there are certain recommendations that should be highlighted for immediate attention:

- **National ICT Strategy.** It is essential that a digital transformation strategy for Kiribati will be developed in cooperation with all stakeholders (public sector, private sector, academia, civil society).
- **Digital government coordination structure.** It is essential to establish a cross-government coordination structure with a clear and widely accepted mandate and statutes. This coordination structure should set the roles and responsibilities of stakeholders. All Government of Kiribati ICT projects should be initiated, prioritised and approved through this structure. It should also oversee the setting up and enforcement of technical specifications for standardisation.
- **Base registers.** It is essential to digitise business processes and create the main set of base registers for population, business and land for Kiribati.
- **Interoperability framework.** It is essential to create a national interoperability framework for Kiribati and, based on this, develop the interoperability solution for secure data exchange. The interoperability framework document should define the approach for delivering public services in Kiribati in an interoperable manner, together with basic interoperability guidelines in the form of common principles, models and recommendations.
- **Digital identity.** It is essential to create and agree on a Kiribati digital identity concept with related general architecture and develop the related digital identity solution.

When implemented, these five essential recommendations will serve as catalysts to achieve results related to all other recommendations presented in the current report.

1. General project overview

The goal of this project is to establish a basis for the staged introduction of digital government systems and facilities for improved internal government efficiency and delivery of government services to an increasingly connected business community and society in Kiribati.

Specific tasks of this project are:
Part 1: Establishment of a Digital Transformation Office[1]
Part 2: Use of existing ICT infrastructure and proposing appropriate new or updated infrastructure
Part 3: Digital government systems

The project duration is 2 years from 01 April 2019 until 31 March 2021.

During the project, the following reports were delivered already:

1. Report 1 - Inception Report
2. Report 2 - Report of a structure of the new office of the CIO (Digital Transformation Office)
3. Report 3 - Report on applications for enhanced efficiency of internal government business functions to run on the network
4. Report 5 - Draft Project documents for Government Network
5. Report 6 - Draft Project documents for Government Data Centre

The current report, as a deliverable of Part 3 (e-Government systems), takes into account the outcomes from the previous tasks and reports, and draws the Digital Government Master Plan and Implementation Plan.

This report sets the principles and enablers of realising digital transformation in Kiribati. The report reviews the current situation and outlines the actions, high priority projects and high value initiatives that can lead to the adoption of modern digital government operations. The masterplan outlines the general principles for developing digital governance and provides some examples for specific initiatives, based on which detailed sectoral plans should be further developed.

The project is implemented by e-Governance Academy Foundation (eGA). eGA is a non-governmental, non-profit organisation, founded for the creation and transfer of knowledge concerning e-governance and digital transformation. eGA implements that mission through training, research, consultancy and change management support. eGA has worked with more than 200 organisations, trained more than 5500 e-government leaders and has been involved in e-governance development in more than 130 countries.

[1] Initially, in the project documents the unit was named CIO Office, according to the discussions with the Kiribati Government the name was change to Digital Transformation Office that is better reflecting the mandate and scope of the work of this unit.

1.1. Objectives

The aims of the project were the following:

Create a development plan that:

- identifies user needs for improved efficiency of internal and inter department government processes and outlines key issues to be addressed to realise the improved efficiencies;
- identifies user needs for the delivery of Government services that are of high value to the economic development and social needs of Kiribati and amenable to improved delivery through digital government ;
- categorises the proposals for the future into the following sample groups:
    - Activities necessary to strengthen the new Digital Transformation Office to direct further work toward setting the foundation and infrastructure (including data standards, enterprise wide architecture, cyber security), processes, and procedures (procurement, contracts and program management) needed to roll out the full digital government initiative;
    - Actions that can be implemented easily and quickly toward the dual goals of improved internal efficiencies and efficient delivery of Government services to business and individuals;
    - High priority (high value and return on investment) projects that may require adaptation of administrative and IT systems but which can be addressed in 2 – 4 years; and
    - High value initiatives that will require adaptation and investment appropriate to a five or more years timeframe.

- Sets out estimates of budget and timeline for each component of investment and work;

1.2. Methodology

The project was implemented based on the following methodology:

- Preliminary research into existing documents (policy documents, strategies, laws, roadmaps, technical architecture documents, Government of Kiribati's agenda, etc.).
- E-governance questionnaire developed by eGA, mapping the existing digital governance situation in Kiribati in the following areas:
    - E-government organisation
    - Infrastructure
    - Legislation and strategy
    - State databases and information systems
    - Digital identity management, digital signatures and trust services
    - Interoperability framework

    - E-government development priorities
- Expert missions and face-to-face meetings with key stakeholders.

1.3. Master Plan structure

The current Master Plan and Implementation Plan cover important topics that are needed to build up digital governance in Kiribati. For the successful implementation of digital society, the Government of Kiribati should pay attention to all topics covered in this report. Still, the implementation can be phased depending on priorities and available resources (including financials).

Chapter 2 covers the general overview of the current situation in Kiribati. Chapter 3 describes the general reference architecture of any advanced digital government. A phased implementation is suggested in Chapter 4 with the immediate need to start digitalisation of the business processes in government agencies. Chapter 5 lists critical enablers for the implementation of the Master Plan.

The Master Plan document is extended with the Implementation Plan spreadsheet. The Implementation Plan sets the potential timeframe and financial estimations for the required actions. It is assumed that the implementation plan fulfilment starts from the beginning of 2020. In case of a delay, the Implementation Plan timing should be adapted accordingly.

2. Digital government development in Kiribati

2.1. Introduction

The Ministry of Information, Communication, Transport and Tourism Development (MICTTD) is tasked to coordinate and implement the digital government in Kiribati, ensuring that the aspirations of the Government with respect to digital government are fulfilled. MICTTD had drafted a high-level roadmap for e-government that identifies key development challenges such as human capacity, inefficient services, budget constraints, data fragmentation, network operating in silos, cyber security, infrastructure and others. The draft e-government Roadmap was approved by the Cabinet on 13 March 2017 and forms the basis for the need for a technical adviser that will guide the Government toward the adoption of modern e-government based operations.

The Government of Kiribati is committed to transforming the delivery of public services, improving government-to-citizens (G2C), government-to-businesses (G2B) and government-to-government (G2G) interactions, which will ultimately enhance good governance.

The current Master Plan and Implementation Plan provides a practical overview of the strategic components of digital society, based on international experience, along with proposals for sectorial interventions. It also provides elements for a communication strategy and an overview of capacity requirements for realising the plan.

This document emphasizes the importance of cooperation and data sharing between existing databases and digital government applications. It is certainly efficient to have a set of reusable digital government components, which all government systems can use. Such components can not only increase efficiency, but also increase service delivery quality.

The main prerequisite for the fulfilment of the proposed Implementation Plan is the availability and readiness of the Kiribati officials and technical experts. This Master Plan and Implementation Plan largely depends on the capability of local knowledge, skills and implementation capacities.

As recognised by Pillar 3 of the KV20, improving ICT access and development will play an important role by facilitating connectivity and accessibility to economic infrastructure. Improving the national ICT infrastructure will support and enhance other drivers of growth.

Indeed, it is important for a citizen-centred and service-oriented state to make sure that various organisations and information systems across the government are able and willing to work together and exchange information.

3. Main building blocks: reference architecture

This chapter describes a general conceptual model and main building blocks of digital governance. The model describes a unified system, which combines existing databases and different distributed autonomous digital government applications into an **integrated digital government system**.

Building of the digital government is an extensive task. Therefore, not to make it more complex, it is reasonable to build a set of reusable components, which all government systems can use. Using such components can save money, but also increase efficiency and service quality.

The main enablers of an integrated digital government are:

1) Digital services to the citizens
2) Interoperability and secure data exchange
3) Digital identity (eID) and trust infrastructures
4) Base registers
5) Metadata management of government systems

The key concept of the general conceptual model is the **single data collection (once-only) principle**. The proposed model ensures the principle that information is supplied to information consumers only once from the source responsible for handling the information and there is no other information source for the same information. According to the “once-only” principle, public bodies should take action to share data with each other, respecting privacy and data protection rules. This calls for a generic and scalable solution to interconnect different systems.

The model handles **society as a service-centred organisation**, which means that all the activities of officials, entrepreneurs, citizens and software/information system are viewed as services. End users (citizens and businesses) see services from a joint service room. They are not interested in the organisation that provides the service, but in the service itself. Although the private and public sector act according to fairly different business rules, the users of their services are the same. Hence, it is practical that the private and public sector develop and manage the services jointly.

In public sector information systems, **front-end and back-end systems should be architecturally clearly separated**. All public sector registers and databases are considered to be “back-end systems”. The task of back-end systems is data management and provision of network services; they do not deal with authentication and authorisation. Hence, there is no need to build components of end user's authentication and authorisation into back-end systems. Web services of back-end systems are made available for the end-user only through service intermediaries (front-end systems).

A full component-based service model for public administrations allows the establishment of public services by **reusing, as much as possible, existing service components**. Public administration institutions should agree on a common scheme to interconnect loosely coupled components and put

the necessary infrastructure in place. The general conceptual model below is based on the experiences with interoperability frameworks of Estonia, European Union, and other relevant samples.

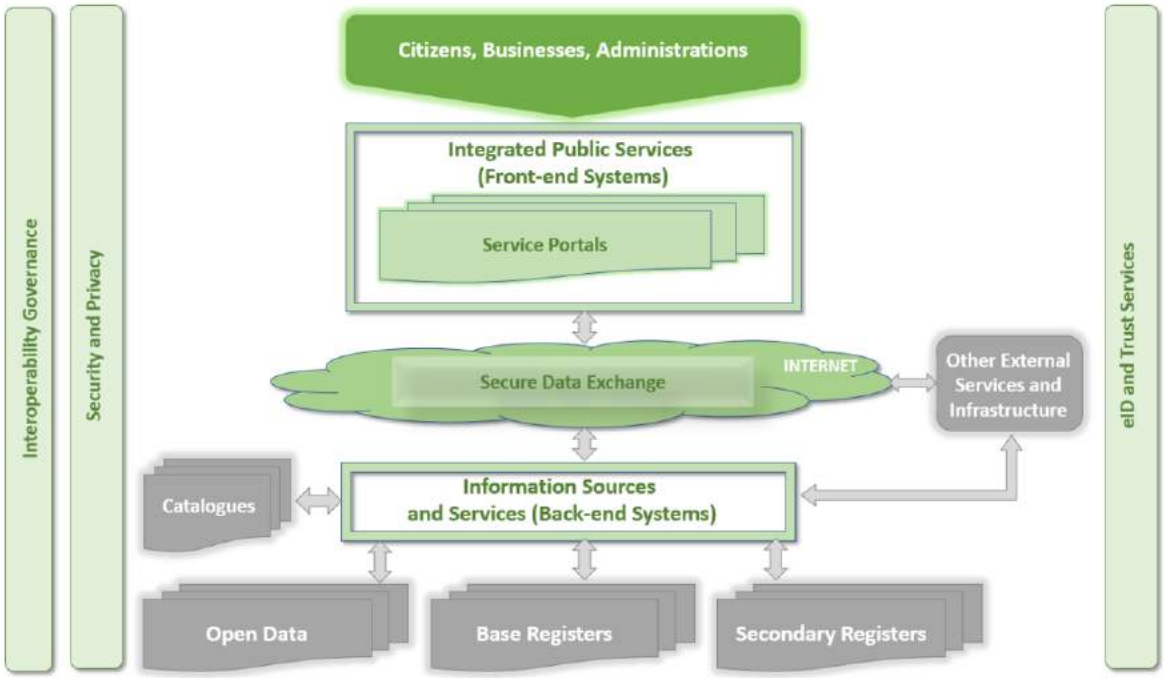

Figure 1. Conceptual model of an integrated digital government

The conceptual model described above does not predefine the architecture or technical approach of the autonomous applications. Regulation comes into effect only when information must be shared. However, a set of regulations are still needed for the general functioning of the system, such as legislation on data protection, archiving, quality management, etc.

The main components of this model are:

- **Base registers.** These are identified as being a trusted and authoritative source of information, which can and should be digitally reused by others and in which one organisation is responsible and accountable for the collection, usage, updating and preservation of information.
- **Secondary registers.** These can contain own master data and master data from base registers transferred over a secure data exchange layer. From the consumer point of view, there are no differences between base registers and secondary registers. A secondary register can contain data transferred over a secure data exchange component from the base registers.
- **Open data.** Public authorities should allow for effective use of data by publishing raw data in a machine-readable format, so that it is available for reuse to any interested party (e.g. for data analysis or creation of applications and services).
- **Catalogues.** These describe reusable services and other assets to increase their findability and usage. This component allows publishers to document and make available resources for reuse by others. Various types of catalogues exist, for example directories of services, libraries of

software components, open data portals, register of registers, metadata catalogues and catalogues of standards.

- **Electronic identity (eID) and trust services.** Infrastructure for digital identification, signing, encryption, sealing, timestamping, certificates validation.
- **Other external services**. Public administration institutions should exploit services provided outside the boundaries of public administration by third parties, such as, payment services provided by financial institutions or connectivity services provided by telecommunications providers.
- **Secure Data Exchange.** All data exchanges must be done in a secure and controlled way. This component is the most crucial factor for the implementation of this model. Internet can be used for secure data transport.
- **Integrated Public Services** allow citizens to access government e-services through portals. Portals should support building complex (aggregated) services and various authentication methods, based on the national system of e-identification.
- **Security and Privacy** should guarantee that information collected about individuals is used only for purposes for which it was originally supplied. Also, citizens and businesses must be assured that they interact with public administration in an environment of trust and in full compliance with relevant regulations.
- **Interoperability Governance** refers to decisions on interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability.

A detailed description of those components is presented in Annex 1. As this model is based on the experiences of Estonia, European Union, and other relevant samples, we suggest that the realisation of an integrated digital government system in Kiribati follows a similar model.

4. Kiribati Digital Government Master Plan and Implementation Plan

The Kiribati Digital Government Master Plan and Implementation Plan focuses on three large areas – governance, technical infrastructure and digital government applications. It is obvious that it is not possible to implement different frameworks and building blocks at the same time. Therefore, the tasks are in different priority levels – H-high, M-medium and L-Low. Also, in every task there are planned activities, expected deliverables, estimated timeline, responsible stakeholders, estimated costs and resources/skills needed.

Some tasks are continuous (like processes) and some have a fixed scope (project type of activities). For example, the Digital Transformation Office will be established during a certain timeframe (as a project), but the execution of tasks of the office is a continuous process. In the same way, policy and legal framework development is a project, but further development should be considered a process.

The Kiribati Digital Government Master Plan and Implementation Plan is based on the assumption that governance is the main enabler of the digital transformation. Governance facilitate the high-level digital transformation process described in Figure 2 below.

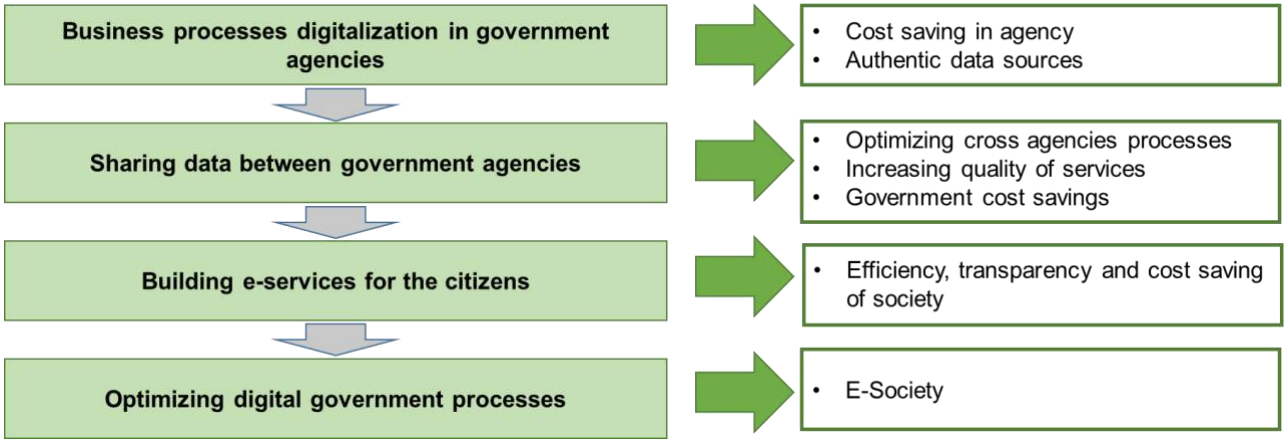

Figure 2. High level implementation plan

Every government agency can start developing digital solutions by optimising their business processes immediately upon available resources. The goal of the digitalisation is to save costs inside an agency and create authentic data sources (registries) which can be shared with other government agencies.

When there are reliable data sources available, the interoperability solution can be built up to optimise business processes cross those agencies. This secure data exchange platform is standardised and universal, so the next data sources can be connected and business processes can be implemented gradually.

Once reliable digital processes and data sources in agencies are available, online services for the citizens can be built. Through e-services, the government services quality will increase remarkably.

When most of the government agencies have digitalised processes and data sources, it is possible to start optimisation of the government business processes and build e-Society as the target. Those new business processes can be built up as proactive life-event-related processes where the initiator of the processes is the government, not the citizen.

All those process steps can run in parallel, but every step needs availability of at least some elements of the previous steps. The organisational, policy, legal, financial and other related issues must be solved in parallel.

4.1. Governance

The Governance category in the Digital Government Master Plan and Implementation Plan is the most important category and enabler for the other categories. In this category, the organisation, policy, legal, financial and awareness related activities should be planned and executed.

4.1.1. Organisation

Planned activities: ***Development of a Digital Transformation Office for sustainable digital government coordination and implementation***
Priority: High
Deliverables: Clearly defined principles, process descriptions, legal acts on establishment of the Digital Transformation Office. recruitment of staff, training of staff
Estimated timeline: 6 months during 2020, afterwards continuous adjustment
Responsible unit: MICTTD, ICT department; Digital Transformation Office once established

There is a great need to develop a Digital Transformation Office that supports and implements cross-government solutions and coordinates the digital transformation in Kiribati.

Horizontal coordination of the nation-wide digital government planning and activities is currently weak or missing. All ministries and other government institutions have their ICT departments, reporting only to their Ministers and Secretaries.

The ICT staff of the ministries and other government institutions is limited and focusing mainly on hardware and local networks maintenance. There is a lack of ICT staff able to develop and maintain software solutions. ICT sector in the country is very limited and providing only hardware sales services, no local software development companies are available.

A prerequisite for the fulfilment of the Implementation Plan is a well-functioning, competent and motivated coordination institution and ICT management of the institutions themselves. Without competent ICT staff in the government, it is not possible to outsource technology development either. Efficiency of development is widely based on competent decisions of public administration officials. ICT management is directly connected to change management in public administration and therefore, it should be coordinated by the top management of the administration.

Coordination mechanisms and organisation need to be further strengthened, competences and roles of the CIO need to be agreed upon and training for IT staff organised. Potential ICT governance model is presented in Figure 3 below.

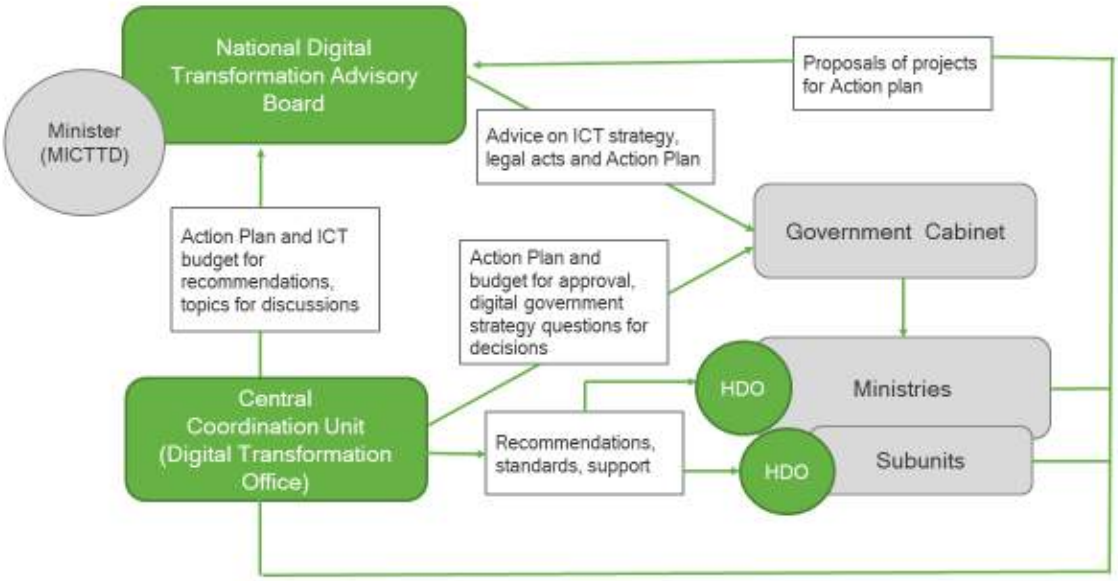

Figure 3. Proposed ICT governance model

Description of the roles and responsibilities

Officer of the Digital Transformation Office

1. Responsible on **ICT strategy planning, implementing and supervising** processes. **Public relations activities** on digital transformation issues.
2. Responsible of development of National ICT Policies and implementation.
3. Responsible for development **cyber security policy**.
4. Have rights to get **information from government bodies about the needs and use of ICT systems**.
5. Responsible for Interoperability Framework and ICT architecture. Coordination of ICT standardisation activities.
6. Responsible on **drafting the ICT budget in state budget** in cooperation with Ministry of Finances. Digital Transformation Office is supervising and, if needed auditing ICT systems development projects.
7. Responsible on coordination of **drafting of main ICT and information society related legal acts.** Office should have right to present opinion and approve all ICT related legal acts.
8. Have right to **initiate new ICT-related legal acts**.
9. Is responsible on planning and implementing **training and awareness raising activities**.
10. Coordinate the **international cooperation** activities in the field of digital transformation and ICT
11. Initiate and coordinate national and **cross-government ICT projects** and programmes.
12. Administrate and support digital government technical solutions, including infrastructure and applications.

13. **National cooperation** on digital transformation with various stakeholder groups – academia, banks, telecoms, various other user groups
14. **Recruitment** of **ICT staff.**

Help Desk Officers (HDO) of the Ministries

The Central Coordination Unit (OGCIO) needs to have contact points in ministries to cooperate with them. Contact points (HDOs of the Ministries) should be assigned on behalf of ministries with the following responsibilities:

- Plan and prepare for approval the annual ICT budget for the management of the ministry The ICT budget should be in line with both the government ICT action plan and the ministerial action plan;
- Cooperate with central CIO in regard to implementation of different projects on Ministry and cross government level, supervision of projects, ICT training issues of ministries, etc.;
- Organise ICT systems maintenance and user help desk;
- Organise end user training on ICT issues.

The Ministry level contact points (HDOs) should be members of the ICT workgroup of ministries led by the Central Coordination Unit (Digital Transformation Office). If agreements reached between ministries, DTO can cover several ministries. Still, as DTOs responsibility is also stand for the ICT budget and action plan in specific ministry he/she should have good reason to work for several ministries.

National Digital Transformation Advisory Board

The National Commission of Digital Transformation is an advisory body for the government, giving opinions and making recommendations to the government and Minister for Information, Communication, Transport and Tourism Development. The Board is led by the Minister for Information, Communication, Transport and Tourism Development. The members are from civil service, academic institutions and private sector. It is important that members of the Board are opinion leaders in the field. It is advisable that the Board also fulfils PR functions on digital transformation issues.

The National Digital Transformation Advisory Board:

- Provides opinions and advice on basic and strategy issues on ICT
- Provides opinions and makes recommendations about ICT-related legal acts
- Monitors the progress of the implementation plan fulfilment semi-annually and gives recommendations in case of deviations

4.1.2. Policy

Planned activities: ***Development of ICT policy, Interoperability Framework, Interoperability Architecture***
Priority: High
Deliverables: National ICT policy. Kiribati Interoperability Framework and Interoperability Architecture
Estimated timeline: 12 months plus during 2020, afterwards continuous adjustment
Responsible unit: Digital Transformation Office

Political leaders must support all necessary digital government development processes to bring about actual change. Political will includes ensuring high-level political leadership and support that leads to the adoption and implementation of relevant policies and agendas. The introduction of digital government should be a political priority and political will must be declared at the highest possible political level. To have proper effect, it is important to identify roles and determine responsibilities for coordination and implementation.

All stakeholders must be involved in policy development, including encouraging public-private partnership (PPP) and cooperation with academia. In small countries like Kiribati, public-private partnership is especially important. Small countries usually have more challenges in returning the investment on digital government solutions, taking into account the relatively small number of users of the services.

A key requirement set in this implementation plan is following a National ICT Policy endorsed by Cabinet in May 2019 that details a national digital government vision, blueprint and action plan for the realisation of an optimally functioning digital government ecosystem.

Also, the Kiribati Interoperability Framework and Interoperability Architecture should be framed so all parallel developments can understand and use the principles of the future connected government.

4.1.3. Legal framework

Planned activities: ***Review of existing legislation and development of digital government related legislative changes***
Priority: Medium
Deliverables: Harmonized legislation, new legal act about personal data protection, digital signature, data management in public sector, other relevant regulations
Estimated timeline: 2 years plus continuous adjustments
Responsible unit: Digital Transformation Office

While infrastructure, connectivity and affordability of ICT are relevant concerns when developing digital government, its implementation is not primarily focused on technology. Organisational and regulatory issues are often even more important. A new digital mind-set is needed to fully benefit from modern digital technologies: digital data and transactions need to have a legal meaning, data must be reused within the government, and service delivery processes need to be redesigned.

The key legal issues to keep in mind in the context of introduction or further developing the digital government can be summarised to include the following:

- There should be no obstacles to using electronic format for administrative acts;
- Electronic acts should have the same legal force as traditional acts;
- There should be a possibility for secure electronic identification and signature;
- Data protection provisions should be in place and implemented;
- There should be rules for the establishment of databases and interoperability of the data;
- Responsibilities for the adoption of necessary rules and regulations should be clear.

The above-mentioned needs are currently not regulated or are only partly regulated in the current legal framework of Kiribati. Kiribati lacks the legislative framework to facilitate the development of digital government.

Whether to have one large piece of legislation on digital issues, or to deal with them in various laws, is a matter of choice and legislative style. Once the digital government is more mature, it is often not needed to have specific legislation on digital government or more generally on digital matters, as the form of different acts or actions will be less important than their content.

The actual legal work for introducing or enhancing digital government needs to be adapted to the legal environment of Kiribati, but the steps to be taken and the general outline of work is similar regardless of the setting. The focus should be on enabling new technologies to be used to perform tasks as set out in existing legislation.

Basic principles

- There should not be too much special legislation on digital government, as it risks creating parallel governance structures.
- It is essential to make an overview of existing laws to make sure digital government methods can be used.
- The question of responsibility for carrying out reforms, for controlling the quality and accessibility of services and for receiving complaints is important and should be regulated by the law.
- Data protection rules and a system ensuring the enforcement of such rules should be regulated.

- There must be a form of secure identification on-line, established by law. In case services are to be offered to the public, such identification must be easily available and easy to use.
- Information and communication technology (ICT) law as well as competition law (sector specific and/or general) is important to ensure that proper access to internet is secured, including how to avoid a digital divide due to the lack of equitable access.
- Digital government can be an important tool for ensuring better access to information and encouraging democratic participation, but the technology should be the tool and not the determining factor for how such access and participation is structured.

4.1.4. Financial framework

Planned activities: ***Harmonization of the digital government development to avoid parallel investments. Development of the regulation enabling to define IT related budget in national budget. Agreements with donors to support the action plan and monitor the use of budget.***
Priority: Medium
Deliverables: Clearly defined digital government budget in the state budget framework
Estimated timeline: Permanent process
Responsible unit: Digital Transformation Office

Today most digital government related developments in Kiribati are implemented though projects funded by international donors. One of the main challenges is the continuous financing of running costs of the ICT systems after the investments.

The national budget also describes some digital government related projects, but no central financial monitoring framework for digital government projects exists.

The following steps assist to manage planning and implementation of the budget for IT and related developments:

- Clearly defined digital government budget within the national budget framework. International donors can contribute to this budget. Clearly fixed responsibilities of institutions and persons, clear rules for managing the budget.
- Clearly regulated and defined budget structure in the national budget. IT budget planning should be linked to an approval process which involves all government institutions. Monitoring the use of the budget is done by MICTTD. The main result is saving money.
- Legal regulation, which enables to define the IT-related budget in the overall national budget, must be in place, as well as agreements with donors to support the action to plan and monitor the use of the budget. This mechanism allows to harmonise digital government development,

avoid parallel investments, enable proper planning and role of CIOs, as well as to focus on the main strategic aims of development (Implementation Plan fulfilment).

- The IT budget should be divided into:
    - development costs (new software solutions developments, ICT projects management, procurement of software and hardware, etc.)
    - running costs needed for the operations and maintenance of IT systems (software and hardware updates, additional software components developments, infrastructure costs, support and maintenance agreements, etc.)

4.1.5. Awareness – digital government communication

Planned activities: ***Development of stakeholder awareness, engagement policies and programs.***
Priority: Medium
Deliverables: Awareness-raising programs, engagement policies, training materials, media plans, etc.
Estimated timeline: Permanent process
Responsible unit: Digital Transformation Office

Access to internet through various digital devices is improving, offering a huge amount of information and possibilities. In order to make the most of it – both from the viewpoint of the ordinary citizen as well as that of a government official – it is important to communicate the opportunities and challenges that are linked to a digital society.

Below we provide some direction for how to organise communication activities once the Implementation Plan is approved and there is a need to sensitise people to issues around digital government.

- Create a "Digital Kiribati" digital government development story that gives every participant a concrete and joint vision to follow. Communicate that vision by developing **common talking points** across all ministries and agencies. All communication starts at the level of the highest public officials: President, Minister of Information, Communication, Transport and Tourism Development, etc.
- All communication should be as **simple** (understandable) **and practical** as possible: the messages should be clearly connected to the benefits that citizens, businesses and the state will receive.
- To **build trust**, spokespersons and opinion leaders should be open and precise when it comes to public communication, avoiding promising things or activities the government is not able to provide.

- To popularise digital government among citizens, government leaders should also be the ones leading by example when it comes to the use of digital government tools (e.g. using public appearances in media to talk about how they use e-services, what measures they take to securely browse the internet, etc.).
- Make government communication mobile-friendly.
- Ministries and agencies should be **active in electronic communication**, promoting the possibility of communication by email, and replying timely to online requests.
- Make sure that all government e-services for citizens and government web-sites can be found by search engines using SEO (Search Engine Optimisation).
- **National and regional media** (TV, radio, newspapers) should be used to keep digital government topics actual in the media by providing information about recent developments and educating people on the topic of ICTs (e.g. a specific radio or TV show that covers digital issues, portal or column in the newspaper).
- Increase **digital awareness** among the population and make digital government developments **sustainable** by training different target groups: teachers, citizens, public officials, but also journalists so that they would know how to cover the topic of digital government.
- Make **ICT knowledge part of the education system** to raise a digitally-skilled young generation. ICT education should be included in the school curriculum (primary and/or secondary level) and several opportunities should be available to study ICT at the tertiary education level (incl. vocational education).
- **Engage partners from all sectors**. National Digital Transformation Advisory Board can be as an avenue to raise awareness to private sector

4.2. Technical Infrastructure

The Technical Infrastructure category in the Digital Government Master Plan and Implementation Plan covers the technical enablers of the digital transformation. In this category, the network, Wide Area Network, data center and unified communications system (e-mail) should be planned and executed.

Technology must be integrated into government processes in a sustainable way with proper institutional and legislative support, including training of personnel. Otherwise, there will be few services in place, which leads to a vicious circle, as digital government will be seen as ineffective and it may take years to convince government departments and their legal offices or citizens to use the technology.

4.2.1. Network

Planned activities: ***Implementing government buildings LAN***
Priority: High
Deliverables: Local Area Networks are available in government buildings
Estimated timeline: 24 months plus continuous adjustment
Responsible unit: Digital Transformation Office, ministries

As digitalisation of the business processes in ministries needs connected workstations and other digital resources, local area networks are needed inside those organisations. To build those networks, cabling is needed along with setting up network devices and managing those. As the resources in the ministries are limited and LAN solutions should be unified, procured and managed centrally, the task will be delegated to the Central Coordination Unit (Digital Transformation Office). [2]

4.2.2. Wide Area Network

Planned activities: ***Building and operation of the Government Wide Area Network (GWAN)***
Priority: High
Deliverables: GWAN is planned, documented, procured and deployed. Operations are in use.
Estimated timeline: 8 months for building, later operation.
Responsible unit: Digital Transformation Office, operators

To build a digital government, there are certain infrastructure elements that need to be developed. Government Wide Area Network (GWAN) connects and integrates all of those components. For instance, as the planned datacenter will store and share government data and will be used by ministries to run their information systems and provide online services, the datacenter needs to be accessed and utilized by Government ministries and offices through GWAN. Another objective of the GWAN is to ensure that communication between Government offices will be much more efficient, cost effective and secure. [3]

[2] Detailed requirements for the networks presented in the report “Report 5 - Draft Project documents for Government Network”.

[3] GWAN planning already started and related plan is described in the document “Terrestrial Cable - Project Document final v2.doc”.

4.2.3. Data centre

Planned activities: ***Building and operating a data centre***
Priority: High
Deliverables: Data centre is planned, documented, procured and deployed. Training is conducted for the local operation experts.
Estimated timeline: documentation 6 months, procurement 6 months, implementation 6 months together with the Submarine cable landing station
Responsible unit: BNL, Digital Transformation Office

The main goal for the national data centre is to support services offered by the public sector either to the public sector (G2G) or to other stakeholders, government to business (G2B) and government to citizens (G2C). Such services rely on the underlying infrastructure and operational services often labelled as Government Cloud.

The government data centre will be co-located with the submarine cable landing site. It contains the lowest risk for network connectivity, smaller risks in the delivery of data centre equipment and is the most inexpensive option as the supporting infrastructure (HVAC, UPS, generators, personnel rooms, security, etc.) could be shared.

Data centre implementation should start with the detailed requirements developments as soon as possible, to be ready for the procurement. Basic data centre requirements should be combined with the requirements for the submarine cable landing station.[4]

[4] The datacentre analysis is presented in a separate document "Report 6 - Draft Project documents for Government Data Centre".

4.2.4. Unified communications system for the Government

Planned activities: ***Planning and setting up unified email and VOIP telephony system for Kiribati Government***
Priority: Medium
Deliverables: Unified email system exists, all government employees have Government e-mail address and are able use it. Unified VOIP telephony system is implemented and operational.
Estimated timeline: 6 months for planning and procurement, later usage trainings and improvement of the process
Responsible unit: Digital Transformation Office, ministries

The unified e-mail system for the Government employees allows to use e-mail in a secure and unified manner. Currently many ministries lack their own e-mail systems and use public cloud-based systems like Gmail or others. For a small country, it is economically feasible to implement one communication system delivered and managed centrally.

The unified VOIP telephony system for the Government employees allows to use phones in the secure and unified manner in the controlled technical environment.

Both systems require fast and reliable communication network and server resources in the planned government datacentre. Therefore, the implementation can start after the relevant infrastructure becomes available. Still, the planning should be started in parallel with the other infrastructure projects so unified communication system requirements will be considered.

4.3. Digital Government applications

The digital government applications category in the Digital Government Master Plan and Implementation Plan covers the main supporting enablers of the digital transformation. In this category the registers, digitalization, citizen portal, catalogue of interoperable solutions, open data, secure data exchange, digital identity, trust services and cyber security related activities should be planned and executed.

4.3.1. Reviewing existing and creation of new registers

Planned activities: ***Reviewing the solutions of existing and new registries and systems. Data digitalization and transforming to web service technologies.***
Priority: High
Deliverables: Existing and new registries are available and open for the online web services
Estimated timeline: 6-month reviewing, continuous implementation
Responsible unit: Ministries, MICTTD, Digital Transformation Office

According to the reference model, the key components of the digital government are authentic data sources, i.e registers. Data collected and stored in those registers is a result of the business processes of the relevant authority or authorities. When processes are paper-based, it is almost impossible to make digital registers from the information stored in the paper documents. Therefore, to create digital data sources, the business processes should be based on digital technologies also.

Moving from paper-based processes to the digital, the business processes can usually be re-designed and optimised. As current resources are limited for this task, Digital Transformation Office should take responsibility for capacity building of analytical and technical staff for information systems development.

When implementing new registers, it must be taken into account that those registers must be open to share data with other government agencies who need information from those registers. The requirements for information sharing are regulated by legislation and defined in the Interoperability Framework. Data can be shared by web services.

The primary focus on digitalisation of the registers should be in redesigning the existing **3 base registers**:

1. **Population register** (civil register) in Civil Registration Office (CRO) in the Ministry of Justice
2. **Business register** in the Business Promotion Division of the Ministry of Commerce, Industry & Cooperatives
3. **Land register** in the Ministry of Environment, Lands & Agricultural Development

Supporting business processes for those registers must be digitalised for that.

The content and data capture procedures of the existing base registers will be analysed, starting from population data management. The population register is also basis for many information systems, voters registry and future electronic ID of Kiribati, so the fast development of this component is the most urgent and important topic in the Action Plan.

Clear plan should be set for the digitalisation of other registers such as Health, Driver's License, Vehicle details etc. using the information from base registers. All registers must be open to share data with other government agencies.

4.3.2. Building the citizen portal and e-services

Planned activities: ***Upgrading the citizen portal as a one-stop source to access public sector information and electronic services***
Priority: High
Deliverables: Upgraded citizen portal for information and e-services
Estimated timeline: 6-month information services implementation and 12-month transaction based services implementation followed by continuous development
Responsible unit: Digital Transformation Office, ministries

The government portal must become a one-stop source for all the information citizens and businesses need to know about government services. The portal will also host all available e-services in the future.

The portal consists of information services (information about how the government works and what services it provides) and e-services (services executable directly in the portal). A prerequisite for the development of e-services is the existence of digital data sources, as described in paragraph 4.3.1.

The Kiribati portal is currently under development but the initial prototype is available at: http://www.kiribati.gov.ki/ The portal must be finalised as soon as possible, to avail relevant information. The portal will be integrated with the catalogue of interoperability solutions where a separate section for the government services stores data about those services.

4.3.3. Catalogue of interoperable solutions

Planned activities: ***Inventory of systems and services, identifying gaps, defining priority areas and the action plan (CatIS proof of concept), implemented together with the eID proof of concept to demonstrate the value of eID and the digital signature solution***
Priority: High
Deliverables: Establishment of catalogue. Registered information systems and services.
Estimated timeline: 6-month establishment, 18-month implementation, continuous information update
Responsible unit: MICTTD, Digital Transformation Office, ministries

The catalogue of interoperability solutions (CatIS) is a supplementary instrument for coordination of state information systems, a tool for the development and administration of cross-domain systems and a support system for the maintenance of base registers and master data.

The goal of CatIS is to guarantee transparent, optimal balance and efficient management of public sector information systems. The CatIS is a tool for getting a clear view of the IT resources in the public sector. In the catalogue, the Government will register data about:

- institutions: owners, administrators, developers and consumers of registers and information systems;
- registers and information systems, the content of the datasets;
- services;
- reusable components: semantic assets, guidelines, etc.

A dedicated website "Catalogue of interoperable solutions - CatIS" (https://upmind.ee/ki/catis) is established for gathering data about institutions, systems and services in Kiribati.

Currently, the Catalogue includes data about 35 institutions and 5 information systems. The Catalogue will be the tool for the Digital Transformation Office for coordination and management of the Kiribati Digital Government resources.

4.3.4. e-Cabinet

Planned activities: ***Develop an e-Cabinet solution for preparing and conducting Governmental sessions.***
Priority: Low
Deliverables: Implemented e-Cabinet solution
Estimated timeline: 12-month implementation
Responsible unit: Digital Transformation Office

The implementation of the e-Cabinet solution eliminates the need to print and deliver paper documents for each Cabinet session – a significant benefit for the environment and the taxpayer. E-Cabinet is a closed information system. Only ministers and dedicated officials can read and/or submit data and electronic documents according to their rights. Well before the weekly cabinet session begins, the ministers access the system to review each agenda item and determine their position. They then click a box stating whether they have any objections or would like to speak on the topic. That way the ministers' positions are known in beforehand. Decisions that have no objections are adopted without debate, saving considerable time.

The solution supports the Government's decision-making processes in Kiribati, from the submission of a draft decision by the relevant institution (ministries, agencies, etc.) to the decision by the Government. This solution does not involve decision-making processes for preparing draft decisions within the institutions.

4.3.5. Secure data exchange solution

Planned activities: ***Secure data exchange – Interoperability solution implementation***
Priority: Medium
Deliverables: Implementation of the secure data exchange – Interoperability solution
Estimated timeline: 12 months, followed by continuous business reengineering
Responsible unit: Digital Transformation Office, ministries

Citizen-centred state and service-oriented information system necessitate linking information systems into an integrated logical whole. To make it come true, different organisations and information systems must be interoperable, or in other words, they must be able to work together. Secure data exchange is one of the main needs and priorities in digital government development.

As a first step for the secure data exchange, it is suggested to start with the proof of concept based on Estonian X-Road. This project can be implemented within six months and will provide an overview of how the proposed digital government model would work in Kiribati and fit to the local needs and expectations.

Based on the outcomes from this project, the plan for the full implementation of the secure data exchange should be developed. For the full implementation project, there should be authentic data sources available to connect to the integrated digital government ecosystem.

4.3.6. Digital Identity, trust services

Planned activities: **Assessment of the needs, action plan development and implementation of the Public Key Infrastructure (PKI) and Digital Identity**
Priority: Medium
Deliverables: Implemented Public Key Infrastructure and Digital Identity, Certification Authority (CA)
Estimated timeline: 24 months plus continuous operation
Responsible unit: Digital Transformation Office, ministries

Digital identity is the cornerstone of digital government. Simply by owning electronic identification tools, citizens will be able to carry out secure electronic transactions and take full advantage of digital government, cutting out the paperwork.

Security and privacy concerns are reduced, as citizens and businesses can use their own national eIDs to access services online. Government services become more flexible and convenient, like the ones offered by the private sector. The gains for businesses can be enormous too and lead to a significant reduction in overheads and boosting profits. It can make a difference between expansion and stagnation for small and medium-sized businesses.

For building digital identity in Kiribati, the following three main enablers are prerequisites:

- Unique personal identification number – every citizen should be identified by a unique "digital name", usually number
- Physical media to store digital credentials – certificates. This can be an ID card, a mobile SIM card, a specific application in the smartphone etc.
- Trusted Certification Authority – an organisation with the Public Key Infrastructure to validate digital certificates.

For this complex solution, clear architecture and action plan will be developed first.

4.3.7. Security and Privacy

Planned activities: ***Data security and cyber security strategy and policy development and implementation. Data security framework.***
Priority: High
Deliverables: Strategy and policy document accepted and implemented. Regular assessments, monitoring, audits and testing, follow-up activities; cyber security exercise
Estimated timeline: 12 months plus continuous operations
Responsible unit: Digital Transformation Office, ministries

Define a common security and privacy framework and establish processes for public services to ensure secure and trustworthy data exchange between public administrations and in interactions with citizens and businesses.

The government of Kiribati must guarantee citizens' privacy, and the confidentiality, authenticity, integrity and non-repudiation of information provided by citizens and businesses. The government of Kiribati should ensure that:

- they follow the privacy-by-design and security-by-design approach to secure their complete infrastructure and building blocks;
- services are not vulnerable to attacks which might interrupt their operation and cause data theft or data damage; and
- they are compliant with the legal requirements and obligations regarding data protection and privacy acknowledging the risks to privacy from advanced data processing and analytics.

5. Critical success factors for the fulfilment of the Implementation Plan

Several critical success factors have been identified for the fulfilment of the Implementation plan

- The **capacity and availability of public officials and technical experts** is seen as the main critical success factor for the implementation of the activities described in the implementation plan. Most of the activities (or their preparation) could be started immediately, but require certain technical knowledge and availability of staff. This means that priorities for implementation must be set, staff need to be trained, and new staff recruited. If necessary, external experts can be involved, but it is recommended that the work is done by Kiribati public officials and experts, so that the knowledge would remain within Kiribati's public and private sector.
- **Motivation and retention of staff** is also important, as training new people is time-consuming and costly. Employees working on the implementation plan fulfilment should be well remunerated and offered other available benefits that motivate them to retain their job.
- **Political will and leadership** are essential for the adoption and implementation of necessary policies and plans. It is often also needed to change the daily routines of the officials working in the government. The government and its leaders must be able to change the mindsets of officials at all levels. Political leaders need to stay engaged and commit time and budget to the cause of digital government. At the same time, it is important to have a leader of the process, who would ideally be a visionary/expert from the public sector taking ownership and leading the process of implementation plan fulfilment.
- A clear **action plan, approved by Government of Kiribati,** for the implementation. For instance, high-level decisions on a unique identifier for the population, on further development of a population registry, on the implementation of electronic identification, etc. will significantly help the smooth implementation of the digital governance for Kiribati.
- **Cooperation and coordination** are the key to achieving long-lasting effect. It is important to identify roles and determine responsibilities for coordination and implementation, but also encourage public-private partnership and cooperation with academic institutions.
- A **sustainable financial model** for digital governance is needed to develop and implement digital government and related services. The introduction of digital government will have a cost, even if it will soon lead to savings in other respects, so it is essential that there is adequate provision for the necessary funds in a sustainable manner. Sufficient financing should be provided on a medium- to long-term basis preferably through multi-annual budgeting. Risks arising from cyclical planning of the state budget could be mitigated by allocating a separate budget line in the state financial forecast to the development of digital government.

Glossary

Term	Explanation
Application	Software that is dependent on the services of an operating system
Base register	Trusted and authoritative source of information which can and should be digitally reused by others, where one organisation is responsible and accountable for the collection, use, updating and preservation of information.
Big data	Extensive datasets/collections of linked data primarily characterised by big volume, extensive variety, high velocity (creation and use), and/or variability that together require a scalable architecture for efficient data storage, manipulation, and analysis
Certification Authority	A trusted entity that manages and issues digital certificates and public keys that are used for secure communication in a public network
Cyber security	(A) the security of cyber devices and; (b) security against threats created through the operation of cyber devices. Security usually means a situation where risks are not materialised
Data	Reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing
Data exchange	Storing, accessing, transferring and archiving of data
Digital identification system	…or electronic identification scheme - a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons
Digital identity	A set of data and software, protected with cryptographic means
Digital signature	Signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified
Digital governance	…or e-governance or electronic governance is the application of information and communication technology (ICT) for delivering government services, exchange of information, communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework
Digital government	… or e-government is using the tools and systems made possible by information and communication technologies (ICTs) to provide better public services to citizens and businesses
e-ID	…or electronic identification - a material and/or immaterial unit containing person identification data and which is used for authentication for an online service
e-identification	…or electronic identification - the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person
e-services	Electronic services - library services delivered via electronic means, whether from local servers or provided via networks
Electronic document	Electronic representation of a page-oriented aggregation of text, images and graphic data and metadata useful to identify and

	understand that data, that can be reproduced on paper or other substrates, as well as rendered electronically on display devices, without significant loss of its information content
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign
Encryption	Process of encoding messages (or information) in such a way that only authorized parties can read it
Geographic Information System (GIS)	A system designed to capture, store, manipulate, analyse, manage, and present spatial or geographic data.
Interoperability	Ability of two or more systems or components to exchange information and to use the information that has been exchanged
Metadata management	The administration of data that describes other data, which involves establishing policies and processes that ensure information can be integrated, accessed, shared, linked, analysed and maintained to best effect across the organisation
Mobile-ID	A service that allows personal identification and authentication with a mobile phone
Mobile messaging gateway	Mobile messaging gateway allows a computer to send or receive Short Message Service (SMS) transmissions to or from a telecommunications Network
'Once-only' principle	An e-government concept that aims to ensure that citizens, institutions, and companies only have to provide certain standard information to the authorities and administrations once, whereas by incorporating data protection regulations and the explicit consent of the users, the public administration is allowed to re-use and exchange the data with each other
Open data	Data that can be freely used, re-used and redistributed by anyone without restrictions from copyright, patents or other mechanisms of control
Online Certificate Status Protocol (OSCP)	Internet protocol used for obtaining the revocation status of an X.509 digital certificate
Payment gateway	A service that authorises a user's transfer of funds between financial institutions to sellers without direct delivery of either bank or credit card account information
Personal identification number	Numeric code used to authenticate an identity
Portal	Web-based interface that provides a single access point to dispersed information
Public Key Infrastructure (PKI)	A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption
Secure data exchange solution	Solution that ensure that all data exchanges are done in a secure and controlled way. Transfer mechanisms should facilitate information exchanges that are: registered and verified, encrypted, time stamped, logged
Secondary register	Trusted and authoritative source of information which can and should be digitally reused by others
Spatial governance	Efficient use of spatial data in everyday governance activities
Timestamp	time variant parameter which denotes a point in time with respect to a common time reference
Trust services	An electronic service normally provided for remuneration which consists of:

	(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services
Unique identifier	A unique number or code used by the government as a means of tracking citizens and residents for the purposes of work, taxation, government benefits, health care, and other government-related functions

Annexes

Annex 1: Detailed description of the general conceptual model

This annex present details of a general conceptual model and main building blocks of digital government presented in Chapter 3.

Interoperability Governance

The society operates through people and organisations who provide their services. Interoperability is the ability of making systems and organisations work together (interoperate). Interoperability was initially defined for information technology or systems engineering services to allow for physical information exchange. This term is used in this document in a broader definition, which considers social, political, and organisational factors.

Interoperability is not merely an IT issue but includes very many facets of the information society. The objective of the interoperability framework is to make the operation of the public sector more effective, improving services offered to citizens.

The more concrete objectives of the framework are:

- To contribute to the development of a service-oriented society, where people can communicate with the state without knowing anything about the hierarchic structure of the public sector or the division of roles in it.
- To bring more transparency into information related political decisions of the information system.
- To support co-development of the state information system.
- To create conditions for free competition, based on the agreed framework.
- To reduce public sector IT costs.

There are general principles of good administration that are relevant to the process of establishing public services. These principles are taken over from the European interoperability framework and can be adjusted to fit Kiribati's needs.

Good administration of public services is based on following principles:

1) subsidiarity and proportionality
2) user-centricity
3) inclusion and accessibility
4) security and privacy
5) multilingualism
6) administrative simplification

7) transparency
8) preservation of information
9) openness
10) reuse
11) technological neutrality and adaptability
12) effectiveness and efficiency

The most relevant and general principle is that of subsidiarity. Principles 2-8 handle end-user needs and expectations. Principles 9-12 are oriented at the common activity of public sector institutions.

The **subsidiarity principle** implies that decisions are taken as closely as possible to the public authorities, entrepreneurs and citizens. In other words, central government does not act unless central action is deemed more effective than action taken at local level.

The **proportionality principle** limits central actions to what is necessary to achieve the agreed policy objectives. This implies that the central government opts for solutions that leave the greatest possible freedom for implementation to local authorities.

User-centricity means that public services are provided to serve the needs of citizens and businesses. Those needs determine which public services are provided and how public services are delivered.

The use of ICT should create equal opportunities for all citizens and businesses due to open, inclusive services that are publicly accessible without discrimination. **Inclusion** aims to take full advantage of opportunities offered by new technologies to overcome social and economic disadvantages and exclusion. **Accessibility** aims at ensuring people with disabilities and the elderly access to public services so they can experience the same service levels as all other citizens.

Citizens and businesses must be assured that they interact with public administrations in an environment of trust and in full compliance with the relevant regulations, e.g. on **privacy and data protection**. This means that public administrations must guarantee that the privacy of citizens and the confidentiality of information provided by businesses are respected.

Within the necessary **security** constraints, citizens and businesses should have the right to verify the information that administrations have collected about them and to decide whether this information may be used for purposes other than those for which it was originally supplied.

Multilingualism and linguistic neutrality come into play not just at the level of user interfaces, but at all levels of design of public services. Whenever possible, information should be transferred in a language-independent format, agreed between all parties involved.

Administrative simplification comes from the widely recognised reality that there is a high redundancy when it comes to information provided by citizens to public administrations. Repeated requests by

different administrations for the same information place a similar administrative burden on citizens who waste time compiling data and filling in forms with the same information over and over again.

Citizens and businesses should be able to understand administrative processes. They should have the right to track administrative procedures that involve them and have an insight into the rationale behind decisions that could affect them.

Transparency allows citizens and businesses to give feedback about the quality of public service provision, to contribute to their improvement and to suggest the implementation of new services.

Records and information in electronic form held by administrations for the purpose of documenting procedures and decisions must be preserved. The goal is to ensure that records and other forms of information keep their legibility, reliability and integrity over time and can be accessed taking security and privacy into account.

In order to guarantee long-term **preservation of electronic records** and other kinds of information, formats should be selected so as to ensure long-term accessibility, including preservation of associated electronic signatures and other electronic certifications, such as mandates.

Openness is the willingness of persons, organisations or other members of a community of interest to share knowledge and to stimulate debate within that community of interest, having the advancement of knowledge and its use to solve relevant problems as the ultimate goal. In that sense, openness leads to considerable gains in efficiency. Specifications, software and software development methods that promote collaboration and the results of which can freely be accessed, reused and shared are considered open.

Re-use is key to the efficient development of public services. Re-use means that public administrations confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevancy to the problem at hand, and decide to use solutions that have proven their value elsewhere.

This implies that public administrations must be willing to share their service components with others. Re-use and sharing naturally lead to **collaboration**, i.e. working together towards mutually beneficial and agreed common goals.

When establishing public services, public administrations should focus on functional needs and defer decisions on technology as long as possible in order to avoid imposing specific technologies or products on their partners and to be able to adapt to the rapidly evolving technological environment. Public administrations should render access to public services **independent of any specific technology or product**.

Public administration should ensure that solutions serve businesses and citizens in the most **effective and efficient** way and provide the best value for taxpayer money.

Secure data exchange

All data exchange must be done in a secure and controlled way. This component is the most crucial factor for the implementation of the model.

Security is a primary concern for data sharing and for the provision of public services. Public administrations providing public services should ensure:

- that the complete infrastructure and building blocks are secure by complying with the principles of a privacy-by-design approach;
- that the services are not vulnerable to attacks, which might interrupt their operation, cause data theft or data damage;
- and that they are compliant with the legal requirements and obligations regarding data protection and privacy.

Data sharing mechanisms should facilitate information exchange between administrations, businesses and citizens that are:

- **registered and verified**: both sender and receiver have been identified and authenticated through agreed procedures and mechanisms;
- **encrypted**: confidentiality of the exchanged data is ensured;
- **timestamped**: maintain accurate time;
- **logged**: electronic records are logged and archived to ensure a legal audit trail.

The logical view of the secure service infrastructure components of the government data sharing platform and their interconnection is illustrated below in Figure 5.

The secure data exchange is based on TCP/IP networks. There are two types of members of information systems: service providers (publishers, back end) and consumers (subscribers, front end). An information system can act in both roles at the same time – publish its own data and at the same time consume data published by someone else. The number of members is unlimited. The components of the platform are displayed below in Figure 5.

The most important component of the platform is the gateway. The gateway encapsulates all of the security complexity for the members of the data sharing system. Gateways standardise the processes of message transfer between the members of the data sharing system. Only the sender and the receiver can see the structure and the content of the messages.

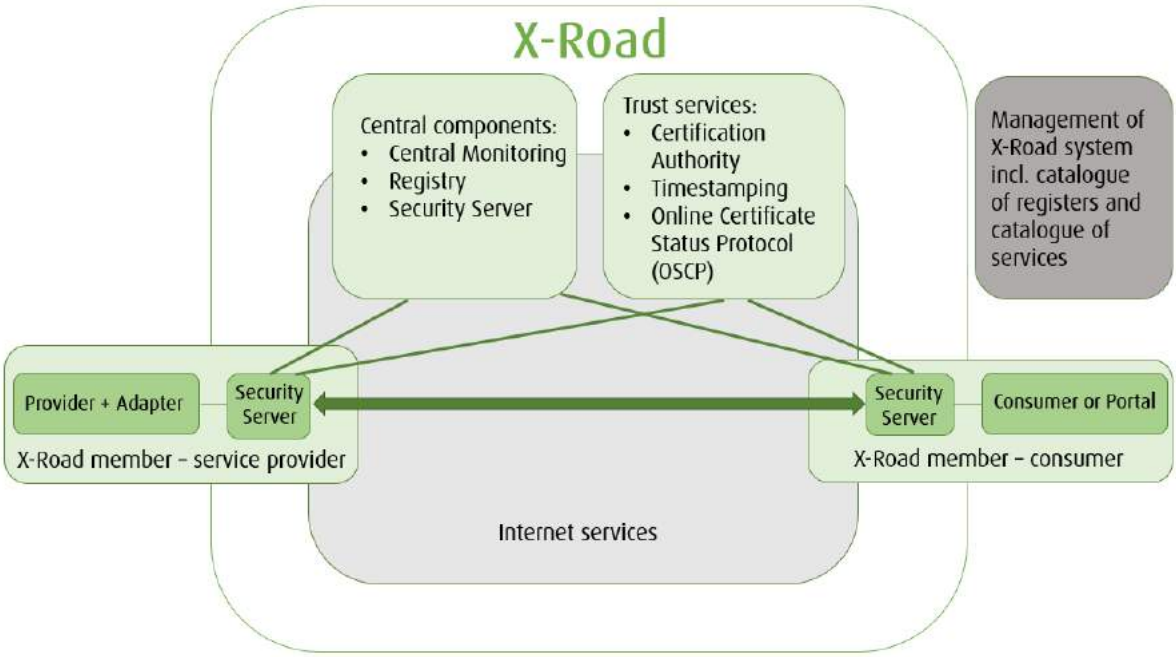

Figure 4. Secure data exchange infrastructure components

The model implies only a minimal amount of central services:

- registry of information systems and services,
- third party identification and authentication,
- transaction log,
- services health monitoring
- and PKI functionality.

Central components provide information to proxy servers about the data exchange participants. These kinds of mechanisms should allow for the secure exchange of electronically verified messages, records, forms and other kinds of information between the different systems. In addition to transporting data, this layer should also handle specific security requirements such as electronic signatures creation and verification, encryption and timestamping. Furthermore, there should be monitoring of traffic to detect intrusions, changes of data and of other type of attacks.

The provision of secure (i.e. signed, verified, encrypted and logged) data exchange via data exchange platform requires several management functions, including:

- Service management to oversee all communications on identification, authentication, authorisation, data transport, etc., including access authorisations, revocation and audit;
- Service registration to provide (subject to proper authorisation) access to available services through prior localisation and verification that the service is trustworthy;
- Service logging to ensure that all data exchanges are logged for future evidence and archived when necessary.

As this secure data exchange model is based on the principle that data is exchanged directly between the data supplier and the recipient without a central intermediator, it does not have a single point of failure. This means there is no single point of risk for a cyber-attack or system malfunction. In case of

failure of one component, other parties can still continue to operate. Also, participants can build their systems at their own pace without waiting for central development.

The secure data exchange model described here has been used in Estonia for more than a decade and we are confident to propose the model for Kiribati as well.

Base registers and secondary registers

A base register is identified as being a trusted and authoritative source of information, which can and should be digitally reused by others and in which one organisation is responsible and accountable for the collection, usage, updating and preservation of information.

Such registers are under the legal control of and maintained by a given public administration, but the information should be made available for wider reuse with the appropriate security and privacy measures.

The most important base registries are registers about persons (population register), companies (business register), land and buildings (land register).

In addition to those, there should be other base registers providing unique and reliable basic information for the all government e-services. Those registers can be:

- Tax register
- Judicial register
- Commercial register
- Deeds register
- Vehicle register
- etc.

There can be many secondary registries which can contain their own master data and data from base registers transferred over the secure data exchange layer.

As base registers are part of back-office functions and can automate internal processes of specific organisations, implementation of base registers can be started without waiting for the availability of other components of the model. Later, upon availability of an interoperability solution, those registers can be published for the relevant consumers.

One of the most important registries – population registry can be built on the existing database in the Civil Registration Office (CRO) in Ministry of Justice. There is also some elements of the land registry existing but no business registry in Kiribati.

eID and trust services infrastructure

Digital identity is the cornerstone of digital government. Simply by owning electronic identification, citizens will be able to carry out secure electronic transactions and take full advantage of digital government and cutting out the paperwork.

Security and privacy concerns are reduced, as citizens and businesses can use their own national eIDs to access services online. Government services become more flexible and convenient, like the ones offered by the private sector. The gains for businesses can be enormous too and lead to a significant reduction in overheads and boosting profits. It can make a difference between expansion and stagnation for small and medium-sized businesses. For example, in Estonia you can set up a limited liability company in just 18 minutes using an eID.

Electronic identification (eID) is the process of using a person's identification data in electronic form, uniquely representing either a natural or legal person or a natural person representing a legal person.

Trust service is an electronic service normally provided for remuneration, which consists of:

a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or

b) the creation, verification and validation of certificates for website authentication; or

c) the preservation of electronic signatures, seals or certificates related to those services.

Figure 6 depicts the conceptual model of eID and trust services infrastructure. A registration authority (RA) is responsible for accepting requests for digital certificates and authenticating the entity making the request. A certification authority (CA) is an entity issuing digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. Validation Authority (VA) is an entity that provides a service used to verify the validity of a digital certificate.

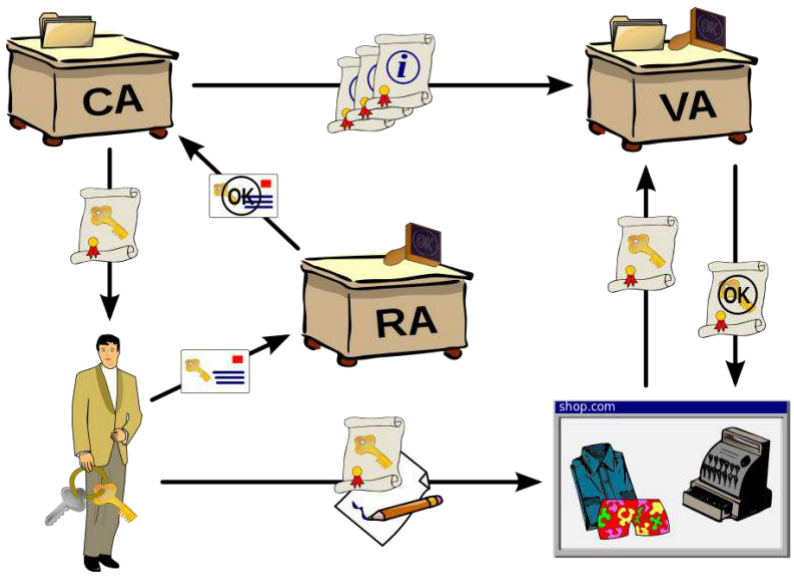

Figure 5. General model of eID and trust service infrastructure

The creation of infrastructure for Kiribati's eID and trust services (KIeIDAS)[5] takes time. While building KIeIDAS infrastructure, ecosystem components should be dispersed as much as possible in the interests of security. Decentralisation ensures transparency of processes and avoids single point of failure risks, which are characteristic of monopolistic, centralised systems. KIeIDAS infrastructure is recommended to be built in partnership with private entities (banks, telecom, certification authorities, etc.) and public institutions (police, ministry of interior, IT coordinating body, IT implementing body, surveillance authority, etc.) For coordination activities, we recommended to establish an inter-agency working group on KIeIDAS infrastructure in Kiribati.

Main activities of the KIeIDAS infrastructure are:

- **Coordination** activities for ensuring interoperability of KIeIDAS infrastructure;
- Preparing **legal regulation** of KIeIDAS ecosystem;
- Issuing ID cards and digital IDs and ensuring they have **qualified certificates** issued by certification service providers;
- Ensuring that citizens have a means, through an activation service, to **link**/**activate** their **eID** with the qualified certification service provider's certificates;
- Issuing **mobile-IDs**;
- Issuing digital IDs for **citizens and resident non-citizens**;
- Issuing digital **seals**;
- Issuing **web certificates**;
- **Supervision** over digital trust service providers;
- Management of the **register** of digital trust services;
- Providing **certification services**;
- Providing **timestamping** services;
- **Digital signing** technology and applications;
- Offering **validation** services;
- Developing and administration of the **digital signature infrastructure.**

[5] eIDAS stands for EU REGULATION No 910/2014 on electronic identification and trust services for electronic transactions in the European internal market: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (25 October 2018)

Metadata management

Catalogue of information systems, services and interoperability assets describe reusable services and other assets to increase their findability and usage. This component allows publishers to document and make available resources with the potential to be reused by others. Various types of catalogues exist, for example directories of services, libraries of software components, open data portals, register of registers, metadata catalogues and catalogues of standards.

The catalogue of interoperability solutions (CatIS) is a supplementary instrument for the coordination of state information systems, a tool for development and administration of cross-domain systems and a support system for the maintenance of base registers and master data.

The goal of CatIS is to guarantee transparent, optimally balanced and efficient management of public sector information systems. CatIS supports the interoperability of databases, the life-cycle management of information systems and re-use of data by providing complete and up-to-date metadata of public sector information systems.

Catalogue components are:

- **Database of institutions**. Provides data about owners, administrators, developers and consumers of registers and information systems. It includes data about important events: registration of institutions, joining institutions to the secure data exchange system, etc.
- **Database of databases and information systems.** This component provides metadata about government registers (DB) and information systems (IS): the name of DB/IS; owner; type of DB/IS; list of services; information about registration and approval; technical architecture; legal acts; service-level agreements; security parameters; logical structure of data (data objects, data fields, parameters of fields).
- **Service repository.** Repository ensures the interoperability of public sector information systems and the reuse of technical, organisational and semantic resources. The service repository is an addition to the metadata kept in the database of databases and includes specifications for all web services and a detailed description of government services (incl. business process descriptions).
- **Repository of semantic assets.** This repository provides information about reusable components: semantic assets, guidelines, etc.

CatIS guarantees the transparency of the state's information system's administration and helps to plan the state's information management.

CatIS provides information on the following subjects:

- Which information systems and databases are implemented in the public sector;
- Which data is collected and processed in which information systems;
- Which services are provided and who uses them;
- Who the responsible and authorised processors of the information systems and databases are,

and who the contact persons are;

- What legal basis the databases are operated on and the data is processed on;
- Reusable components that ensure the interoperability of information systems (XML assets, classifications, dictionaries and ontologies).

CatIS serves as the procedural and administrative environment for the following actions:

- Registration and approval of information systems and databases;
- Registration of services;
- Registration of connections to the secure data exchange (SDE) platform;
- Administration of reusable components (XML assets, classifications, dictionaries, ontologies).

CatIS provides trustworthy assistance and is a great tool for developers, administrators and users of the state's information system. CatIS offers tools for coordinated activities of several bodies. The main stakeholders of CatIS are depicted in Figure 7.

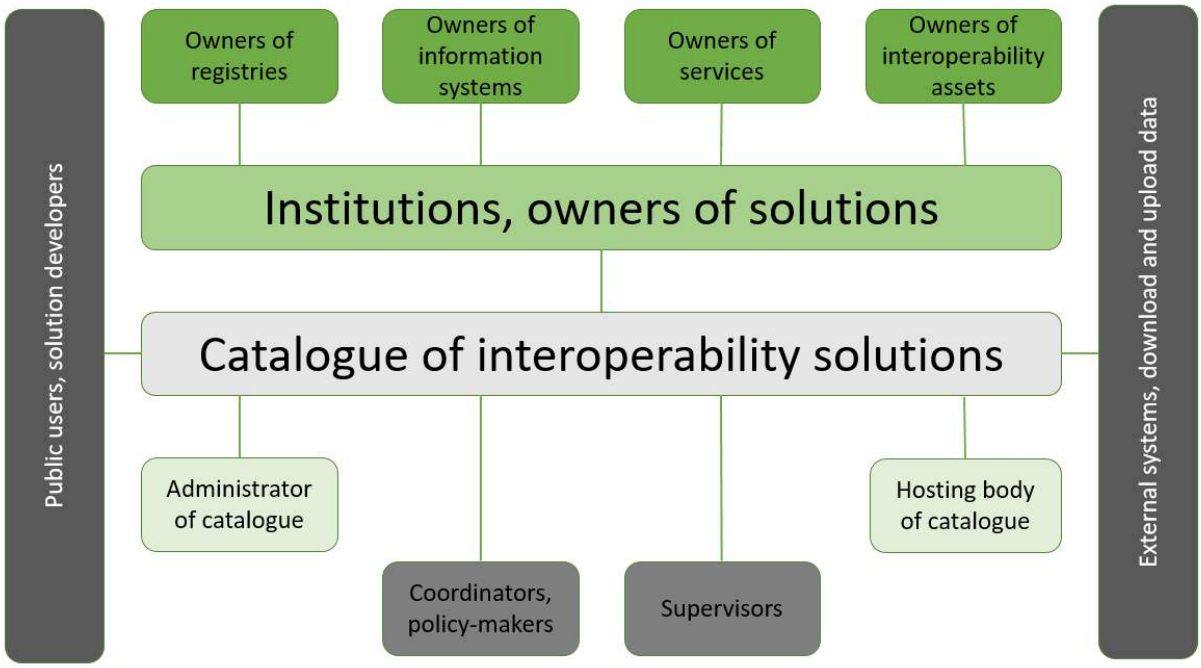

Figure 6. Main stakeholders of CatIS

Stakeholders co-create the content of the catalogue. Experts of institutions submit data about their institutions, owners of registers provide data about their registers, owners of consumer organisations about their information systems, owners of services about their services, owners of interoperability assets about their assets. Coordinators and supervisors use the catalogue and will register their decisions there.

To evaluate the model and understand the basic principles and requirements of metadata management, a short Proof of Concept pilot project can be carried out in Kiribati.

Open data ecosystem

While governments and businesses collect a wide range of data, they do not always share this data in ways that are easily discoverable, usable or understandable by the general public.

To allow for effective use of data, it must be submitted in a machine-readable format; explicit rules should be established for data recycling, ensuring the interoperability of information systems and services. Kiribati should build an open data ecosystem to support data recycling.

The availability of open data will contribute to:

- **Transparency of governance** – involvement of citizens, empowering them and opening research and cultural assets for their use is an obligation of all countries;
- **Innovation** – open data is closely related to open government initiatives and new technology trends, such as open formats, free software, linked information, big data, future Internet and co-creation;
- **Boosting the economy** – opening public sector information will allow private and third sector organisations to combine these with various data and create new business services with added value. It is not easy to appraise the possible monetary influence of data recycling on society, as the influence is largely indirect.

Kiribati needs solutions to the following problems:

- Development and implementation of an open data policy for Kiribati;
- Increasing the transparency of the public sector, transition from the “public by default” principle to the “open data by default” principle;
- Using new knowledge, innovations and services, created on the basis of open data, to enliven the economy;
- Speeding up the transition to future technologies (linked data technologies, Internet of Things, big data and co-creation);

This should go hand in hand with the development of an open data portal for Kiribati.

Kiribati Digital Government Implementation Plan Actions 2020-2023

Document reference	Area	PRIORITY H-high, M-mid, L-low	Planned activities	Deliverable	Estimated timeline	2020/1	2020/2	2021/1	2021/2	2022/1	2022/2	2023/1	2023/2	Responsible unit and stakeholders	Estimated cost (AUD)	Resources/skills needed
4.1. Governance															**$2,625,000**	
4.1.1	Organisation	H	Development of Digital Transformation Office for sustainable digital government coordination and implementation	Clearly defined principles, process description, legal acts on establishment of the CIO Office. Recruitment of staff, training of staff. Office building.	6 months + continuous adjustment									MICTTD, ICT department; Digital Transformation Office when established	$1,500,000	Digital government experts, 10-20 external expert days
4.1.2	Policy	H	Development of ICT policy, Interoperability Framework, Interoperability Architecture	National ICT policy. Kiribati Interoperability Framework and Interoperability Architecture	12 month plus continous adjustment									Digital Transformation Office	$47,000	Digital government experts, 20-30 external expert days (if needed)
4.1.3	Legal	M	Overview of existing legislation and suggestions for digital government related legislative changes	harmonised legislation, new legal act about personal data protection, digital signature, data management in oublic sector etc.	2 years plus continuous adjustments									Digital Transformation Office	$47,000	Legal experts in the field of digital government (data protection laws, contract law, procurement law, fraud, etc.), 10-20 external expert days (if needed)
4.1.4	Financial	M	Harmonise digital government development to avoid parallel investments. Develop legal regulation enabling to define IT related budget in state budget. Agreements with donors to support the action plan and monitor the use of budget.	Clearly defined digital government budget in the state budget framework	Continuous									Digital Transformation Office	$31,000	Financial experts, digital government experts, 10 external expert days (if needed)
4.1.5	Capacity Building & Awareness	M	Development of stakeholder awareness, engagement policies and programmes.	Awareness-raising programmes, engagement policies, training materials, media plans, etc.	Continuous									Digital Transformation Office	$1,000,000	Communication experts, digital government experts
4.2. Technical Infrastructure															**$9,300,000**	
4.2.1	Network	H	Implementing government buildings LAN	Local Area Networks are available in government buildings	24 month plus continous adjustment									Digital Transformation Office, ministries	$2,800,000	Infrastructure project
4.2.2	Wide Area Network	H	Building and operation of the Government Wide Area Network (GWAN)	GWAN is planned, documented, procured and deployed. Operations are in use.	8 months for building, later operation.									Digital Transformation Office, operators	$4,500,000	Infrastructure project
4.2.3	Datacentre	H	Building and operating datacentre	Datacentre is planned, documented, procured and deployed. Training is conducted for the local operation experts.	documentation 6 month, procurement 6 month, implementation 6 months together with the Submarine cable landing station									BNL, CIO Office	$1,500,000	expert on data centre (existing project), procurement expert, experts and administrators of implementation. HW and SW

4.2.4	Unified communications system for Government	M	Planning and setting up single email and telephony system for Government	Single email and telephony system exist so all government employees have Government issued e-mail address and can use it. Also all government workplaces can connect through desktop phone.	6 months for planning and procurement, later usage trainings and improvement of the process									CIO Office, ministries	$500,000	Technical expert, procurement expert. Experts and administrators of implementation and support.
4.3. eGovernment applications															**$6,660,000**	
4.3.1	Reviewing existing and creation of new registers	H	Reviewing the solutions of existing and new registries and systems. Data digitalisation and transforming to web service technologies.	Existing and new base registries are available and open for the online web services	6 months reviewing, continuous implementation									Ministries, MICTTD, Digital Transformation Office	$1,300,000	Procurement experts, enterprise architects, business architects, data architects, solution architects, IT developers, legal experts
4.3.2	Building citizen portal and e-services	M	Upgrading the citizen portal as a one-stop source to access public sector information and electronic services	Upgraded citizen portal for information and e-services	6 month information services implementation and 12 months transaction based services implemenetation followed by continuous development									Digital Transformation Office, ministries	$470,000	Information society experts, project coordinator, IT experts
4.3.3	Catalogue of interoperable solutions	H	Inventory of systems and services, identifying gaps, defining priority areas and the action plan (CatIS proof of concept), implemented together with the eID proof of concept to demonstrate the value of eID and the digital signature solution	Establishment of catalogue. Registered information systems and services.	6 months establishment, 18 month implementation, continuous information update									MICTTD, Digital Transformation Office, ministries	$160,000	Business architect, data architect, project coordinator, 20 external expert days
4.3.4	e-Cabinet	L	Develop an e-Cabinet solution for preparing and conducting Governmental sessions.	Implemented e-Cabinet solution	12 months									Digital Transformation Office	$450,000	Information society experts, project coordinator, IT experts
4.3.5	Secure data exchange	M	Secure data exchange – Interoperability solution implementation	Implementation of the secure data exchange – Interoperability solution	12 months, followed by continuous business reengineering									Digital Transformation Office, ministries	$780,000	Business architect, project coordinator, 4-6 system administrators, 6-10 IT developers, ca 180 external expert days

4.3.6	Digital Identity, Trust services	M	Assessment of the needs, action plan development and implementation of the Public Key Infrastructure (PKI) and Digital Identity	Implemented Public Key Infrastructure and Digital Identity, Certification Authority (CA)	24 months + continuous operations									Digital Transformation Office, ministries	$3,200,000	PKI experts, security experts, procurement experts, legal experts, technology architect, external expert (if needed)
4.3.7	Security and Privacy	M	Data security and cyber security strategy and policy development and implementation. Data security framework	Strategy and policy document accepted and implemented. Regular assessments, monitoring, audits and testing, follow-up activities; cyber security exercise	12 month + continuous operations									Digital Transformation Office, ministries	$300,000	Cyber security experts, 60-100 external expert days