GOVERNMENT ICT STANDARDS

Government Enterprise Architecture

First Edition 2016

The ICT Authority is a State Corporation under the State Corporations Act 446
www.icta.go.ke

CONTENTS

ICTA STANDARDS DESCRIPTION

S/No	Thematic Area	Standards	Brief Description
1	Infrastructure	ICTA-2.001:2016 Network Standard	Provides compliant requirements for design, installations and management of all categories of IT Networks to be deployed in government.
		ICTA-2.001:2016 Data Center Standard	Provides compliant requirements for design, installations and management of government data centers
		ICTA-2.001:2016 Cloud Computing Standard	Provides compliant requirements for design, installations and management of cloud computing infrastructures for government
		ICTA-2.001:2016 End-User Equipment Standard	Provides the minimum specifications for all computing devices being deployed in government
2	Systems & Applications	ICTA-6.001:2016 Systems & Applications Standard	Provides compliant requirements for design, installations and management of all government Software and applications Systems.
3	IT Security	ICTA-3.001:2016 Information Security Standard	Provides compliant requirements for design, installations and management of Information Technology Security in government.
4	Electronic records management	ICTA-4.001: 2016 Electronic records and Data Management Standard	Provides compliant requirements for management of government electronic records and data
5	IT Governance	ICTA. 5.001: 2016 IT Governance Standard	Provides compliant requirements for IT Governance in government. This includes compliance requirements for government IT service providers and Professional Staff.
6	ICT Human Capacity	ICTA.7.001:2016 ICT Human Capital and Work force Development Standard	Provides compliant requirements for development of Human Capital capacity for deployment and support for government ICT infrastructure and services.

REVISION OF ICT STANDARDS

In order to keep abreast of progress in industry, ICTA Standards shall be regularly reviewed. Suggestions for improvements to published standards, addressed to the Chief Executive Officer, ICT Authority, are welcome.

DOCUMENT CONTROL

Document Name:	Government Entreprise Architecture
Prepared by:	Government enterprise Architecture Technical Committee
Edition:	First Edition
Approved by:	Board of Directors
Date Approved:	11th August 2016
Effective Date:	1st January 2017
Next Review Date:	After 3 years

FOREWORD

The ICT Authority has express mandate to, among others, set and enforce ICT standards and guidelines across all aspects of information and communication technology including systems, infrastructure, processes, human resources and technology for the public service. The overall purpose of this specific mandate is to ensure coherence and unified approach to acquisition, deployment, management and operation of ICTs across the public service, including state agencies, in order to promote service integration, adaptability and cost savings through economies of scales in ICT investments.

In pursuit of achievement of this mandate, the Authority established a Standards Committee to identify the critical standards domain areas as well as oversee the standards development process. A total of Nine Standards falling under six different domain areas were identified by the committee to be relevant for government ICT Standards. The development of all the identified standards was done through a process which took into consideration international requirements, government requirements, stakeholder participation as well as industry/sector best practices. In order to conform to the format of other existing national standards, the committee adopted the Kenya Bureau of Standards (KEBS) format and procedure for standards development. In addition, through Memoranda of Understanding, KEBS has made invaluable contribution to the development of ICT Authority standards.

The ICTA GEA has therefore been prepared in accordance with KEBS standards development guidelines.

The Authority has the oversight role and responsibility for management and enforcement of this standard. The review and approval of the standard is done by the ICTA Board upon recommendation of Standard Review Board. The Authority shall be carrying out quarterly audits in all the Ministries, Counties, and Agencies (MCA) to determine their compliance to this Standard.

The Authority will issue a certificate of compliance to agency upon completion of the audit assessment. For non-compliant agencies, a report detailing the extent of the deviation and the prevailing circumstances shall be tabled before the Standards Review Board who will advise on action to take.

All government agencies are required to ensure full compliance to this standard for effective and efficient service delivery to the citizen. The compliance period is six months from the effective date.

Kipronoh Ronoh P.
Director, Programmes and Standards

INTRODUCTION

Strategic management of Information, Information Systems and Information &Communication Technology of the Kenyan Government is key to the overall social economic performance and needs to be closely coordinated across all agencies. MCAs have been using a variety of frameworks and methods to develop ICT plans and implement ICT projects resulting to inconsistency across government and MCAs.

The Government Enterprise Architecture is the means of organising an enterprise's resources i.e its services, processes, information, applications, and technology infrastructure. It establishes a set of policies and technical choices to achieve desired business outcomes, technical standardisation and integration.

To achieve effective enterprise architecture requires the application of a comprehensive and rigorous method for describing a current and future structure and behaviour for the Government's processes, information, applications, technology and supporting human resources. This will enable alignment with current strategic directions.

GEA relates to the practice of business strategy, efficiency and effectiveness. It captures, documents, classifies and analyses all aspects of an enterprise in order to make the information relevant for different types of decision makers.
The Ministry of ICT and ICT Authority constitutes the collective governing body of Information& Communication Technology (ICT).Theyarechargedwiththeresponsibilitytogovern Government-WideICTplansandprogrammes through the GEA. In coming up with the GEA, we were guided by the principles and Values of ICT.(asdepictedinFigure1:ICTHouse of values/pillars).

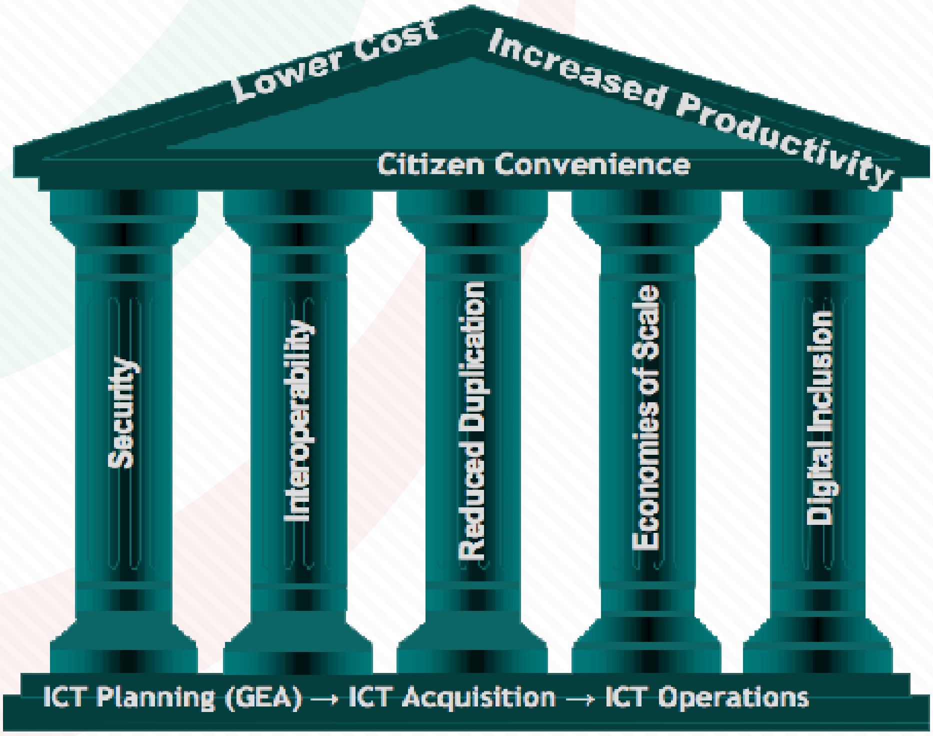


Figure1: ICT Pillars

Heads of ICT departments and the management are strongly advised to conform to above framework, for all initiated ICT projects.
To address the in consistency and misalignment of ICT plans, the ICTA has developed this Government Enterprise Architecture (GEA) Framework as a minimum standard to be used across all government departments and MCAs. The GEA Framework is intended to supersede any prevailingEnterpriseArchitectureandICTplanningframeworksandmethodsinuseingovernment.

The GEA Framework, prescribes a method and defines the minimum components of an ICT Plan, and the subsequent standards will provide sufficient guidelines on how to implement Government. The Government Enterprise Architecture is a mission-focused framework for ministries, its department, and its constitutional bodies to improve government performance. By aligning government's business processes, information flows, and technology consistently across and throughout the Government, the GEA builds a blueprint for improving management of programs.
The GEA Framework supports enterprise architecture activity within the Government of Kenya by defining:

Architecture practices to help drive business management improvements across the Government
the agreed standard architecture abstraction levels across Government
a means to establish a standard and coherent set of classification or domain models of the whole-of-Government enterprise architecture
a set of common artefact types in the form of strategies, principles, policies, standards, requirements and other artefacts used to form the basis of the whole-of-Government target enterprise architecture
a framework within which traditional enterprise architecture artefacts can be accommodated
the means to describe the whole-of-Government target enterprise architecture
mechanisms and tools for alignment with the whole-of-Government target enterprise architecture
the governance and contribution process for the development, use and update of enterprise architecture artefacts.

PURPOSE

The purpose of this ICT implementation guide is to provide direction to Government MCAs and heads of ICT departments to use the Government Enterprise Architecture (GEA) Framework as means to develop an Enterprise Architecture Plan for a department/ or programme of Government. The GEA Framework is generic and can be applied in all spheres and levels of government, and is valuable in developing department/ Enterprise Architecture Plan (also referred to as ICT Plan or ICT Roadmap) that is fully aligned with the department/ business plan, whilst observing the objectives and principles of the e-Government as defined in the ICT House of Values.
MDCAs should use this guide to tailor or establish their EA capability to meet the minimum requirements as contemplated in the GEA Framework.

VISION

The vision of GEA is to provide seamless integration for citizen services empowered through inter-departmental collaboration through ICT standardization

SCOPE AND APPLICATION

The scope of this guide pertains to guidelines on how to implement the GEA Framework in government. It defines the government-wide EA principles, provide guidance on how an EA capability co-exist with other relevant management and engineering capabilities, provides reference models to inform the scope of work and responsibility of an EA development that can be tailored to suite the needs of a department.

NORMATIVE REFERENCES

The following standards contain provisions, which, through reference in this text, constitute provisions of this standard. All standards are subject to revision and, since any reference to a standard is deemed to be a reference to the latest edition of that standard, parties to agreements based on this standard are encouraged to take steps to ensure the use of the most recent editions of the standards indicated below. Information on currently valid national and international standards can be obtained from Kenya Bureau of Standards.

This implementation guide is based on The Open Group Architecture Framework version 9 (TOGAF-9) as tailored by the GEA Framework. It is therefore essential to use the TOGAF-9 documentation as supplementary reference material to this guide.

TOGAF, an Open Group Standard, is a proven enterprise architecture methodology and framework used by the world's leading organizations to improve business efficiency. It is the most prominent and reliable enterprise architecture standard, ensuring consistent standards, methods, and communication among enterprise architecture professionals.

DEFINITIONS AND ABBREVIATIONS

For the purposes of this ICTA Standard the following definitions, abbreviations and symbols apply:

Abbreviations

ADM	Architecture Development Method EA	Enterprise Architecture
GEA	Government Wide Enterprise Architecture	
ICT	Information and Communication Technology	
ISO	International Organisation for Standardisation	
MIOS	Minimum Interoperability Standards	
TOGAF	The Open Group Architecture Framework	
UML	Unified Modelling Language	

Definitions

(Note: Refer to TOGAF9Documentation for more comprehensive set of definitions)

Activity A task or collection of tasks that support the functions of an organization [TOGAF].

Actor A person, organization, or system that has a role that initiates or interacts with activities or a system. [TOGAF]

Architecture (1) The fundamental conception of a system in its environment embodied in its elements, their relationships to each other and to its environment, and the principles guiding its design an devolution.[ISO/IEC42010:2008]
(2)The formal description or blueprint to the fundamental conception of a system in its environment embodied in its elements, their relationships to each other and to its environment, and the principles guiding its design and evolution.[Adapted TOGAF and ISO/IEC42010:2008]

Architecture Domain An architecture focus area within the context of Enterprise Architecture that is concerned with the development to one of business, data, application or technology architecture [Adapted TOGAF.

Architecture Framework A classification scheme that defines the principles, method and deliverables
By which to develop architecture for different stakeholders within an organisation.[Adapted TOGAF]

Architecture Principle A qualitative statement of intent that should be met by the architecture; and contains at least a supporting rationale and a measure of importance[TOGAF].

Application The software product that enables one or more functions or services of an organisation.[Adapted TOGAF]

Application Architecture The architecture of the application (or software)that are needed to process
The data and enable one or more functions or services of an organisation. [TOGAF]

Baseline Architecture The existing or an architecture that is used as a basis for transformation or change [Adapted TOGAF].

Business Architecture The architecture of the business strategy, organization structure, functions/services, key business processes and information requirements, as well as the relationships between these concepts. [Adapted TOGAF]

Business Service The output of a capability.

Capability (1) An arrangement of business resources (means) that is able to produce a product or render a service, where resources usually include people, competencies, processes, information, information technology and machines.[Adapted TOGAF]
(2)The inherent function(s) of computer hardware or software

Deliverable A work product (output) of a particular step in an architecture development method.[Adapted TOGAF]

Data A collection of facts usually collected as the result of experience, observation or experiment, or processes within a computer system, or a set of premises. This may consist of numbers, words, or images, particularly as measurements or observations of a set of variables. Data are of ten viewed as a lowest level of abstraction from which information and knowledge are derived.[Wikipedia]

Data Architecture The architecture of the data resource inherent to an information system. [Adapted TOGAF]

Enterprise The highest level of description of an organization and typically covers all missions and functions. An enterprise will often span multiple organizations .[TOGAF]

Enterprise Architecture The Business, Data, Application and Technology Architectures required to enable and support the Enterprise emissions overtime; including baseline architecture, target architecture, and an implementation plan.[Derived TOGAF]

Information Technology(IT)

A general term use to refer to one or more of the subject are as relating to the computer industry, such as Business Continuity, Business IT Interface, Business Process Modelling and Management, Communication, Compliance and Legislation, Computers, Content Management, Hardware, Information Management, Internet, Networking, Programming and Software, Security, Standards, Storage, Voice and Data Communications.[Adapted TOGAF]

The name of the department within an organisation that are tasked with responsibilities to provide computer related or information management services to the organisation.[Adapted TOGAF]

Function

A specific task or set of activities that an organisation is designated to perform.

Computerscience:thespecificactionortaskthatapieceofsoftwareisdesignedtoperform.[Wikipedia]

Computer engineering: the specificaction or task that a hardware system or subsystem is designed to perform.[Wikipedia]

Infrastructure Infrastructure is everything that supports the flow and processing of information.

Interoperability (1)The ability to share information and services.[TOGAF]

(2)The ability of two or more systems or components to exchange and use information.[TOGAF]

Model A representation of a subject of interest (view)that addresses the concerns(viewpoint) of a particular stakeholder.[Adapted TOGAF]

Organisation A self-contained unit of resources with line management responsibility, goals, objectives, and measures. Organisations may include external parties and business partner organisations [TOGAF]

Roadmap An abstracted plan for business or technology change, typically operatingacrossmultipledisciplinesovermultipleyears. Normally used in the phrases Technology Roadmap, Architecture Roadmap, etc.[TOGAF]

Target Architecture The future state (to-be) architecture for an organisation or system.
Technology Architecture System
TOGAF The architecture of the foundation software, hardware and telecommunications capabilities that are required to enable processing and deployment of business ,data, and application services, which includes application processing infrastructure services, naming and directory services, middleware, database management infrastructure, telecommunication network infrastructure, computer hardware, storage and peripherals, security infrastructure, system management infrastructure and interoperability standards[adapted from TOGAF]

Systems that are man made and may be configured with one or more of the following: hardware, software, data, humans, processes (e.g. processes for providing service to users), procedures (e.g. operator instructions),
software products and services; and
Software-intensive systems "any system where software contributes essential influences to the design, construction, deployment, and evolution of the system as a whole" to encompass "individual applications, systems in the traditional sense, subsystems, systems of systems, product lines, product families, whole enterprises, and other aggregations of interest" .
The Open Group Architecture Framework. TOGAF is an architecture framework that defines the methods and tools for assisting in the acceptance, production, use, and maintenance of enterprise architecture. It is based on an iterative process model supported by best practices and are usable set off existing architecture assets.[TOGAF]

REQUIREMENTS

Government coordination depends upon consistent decision making across multiple departments and projects. But a natural tension exists whenever more than 25 ministries and their departments must work together as one. An enterprise-wide architecture tries to create a framework for effective decision making across multiple departments. Otherwise, independent groups decide alone resulting in inconsistency, information islands, isolated business processes, and inefficient technologies. This mixture is a recipe for poor performance.

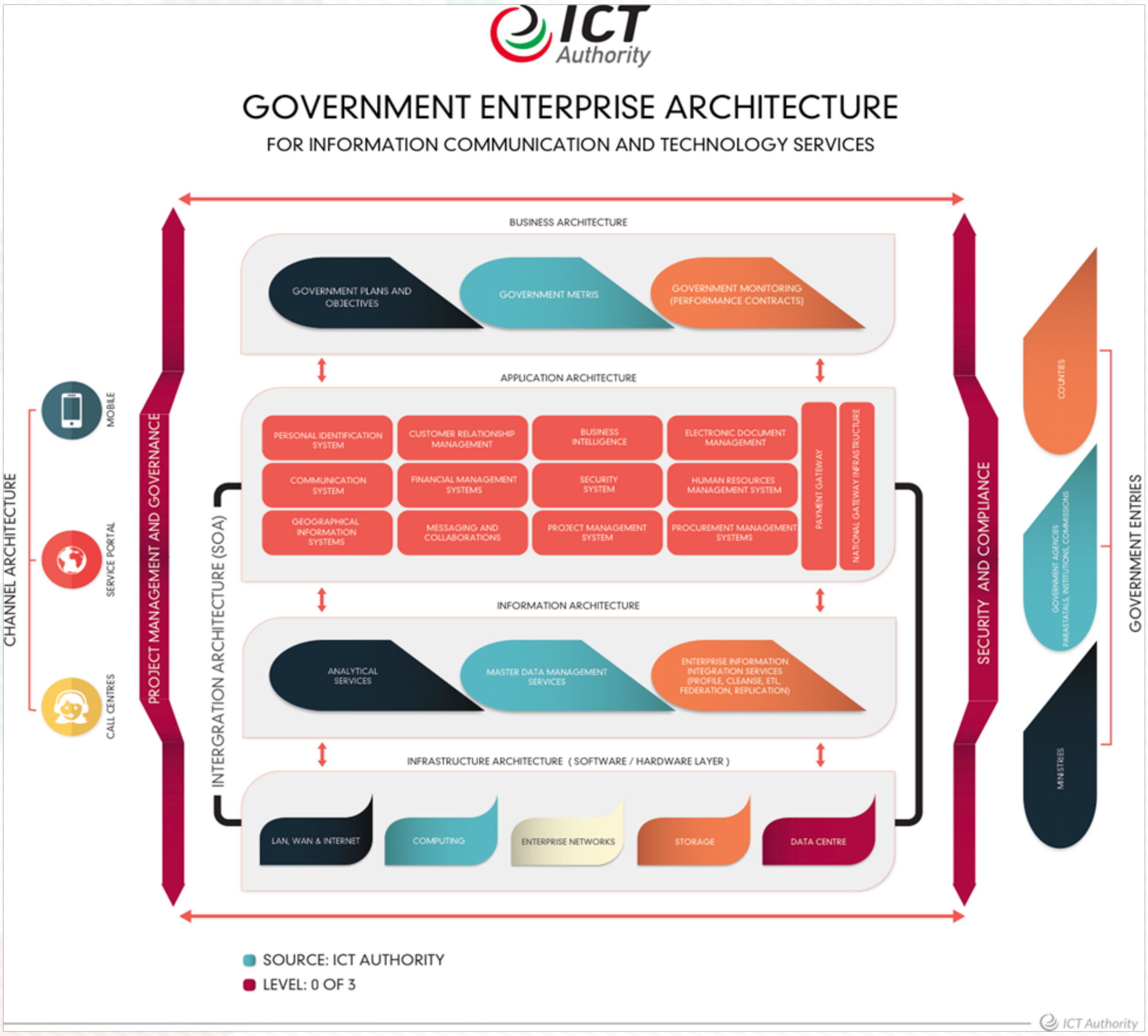
PRINCIPLES

Principles are general rules and guidelines, intended to be enduring and seldom amended, that are used to govern and guide the way in which an organization sets about fulfilling its mission.
The Kenyan Government Enterprise Architecture Principles ('principles') are based upon addressing the importance of getting results, obtaining maximum return-on-investment and cost efficiency of operations, providing quality information and technology, protecting privacy, maintaining secure information, and providing service to the public.

The principles, as a key enabler for whole-of-government outcomes, will contribute to aligning and cross- services and solutions with goals and strategies at both the and whole-of-government levels. The principles should form not only part of the EA capability of Government MCAs, but also the systems life cycle, capital planning and investment decision-making processes at the , cross- and whole-of-government levels.

MCAs should adapt the principles to meet their specific business needs, through mapping of specific actions (such as EA development, business initiatives, ICT acquisitions and implementation) to the principles. The principles relate to the delivery of business services undertaken by the Government, and should not be seen as being constrained to the delivery of information and communications technology (ICT) related services.

Enterprise Architecture principles are used to govern and guide enterprise architecture development and trade-off decisions (i.e. strategic planning, alignment, investment and macro design) of Information and ICT, whereas Solution Architecture principles are used to govern and guide the mission of Software and System development (e.g. requirement analysis, technical design, construction, procurement, integration).
This set of principles pertains to Enterprise Architecture and must be observed when developing and reviewing Enterprise Architecture for Government. These principles may be expanded and unpacked into Solution Architecture principles (as depicted below.


ICT Authority
GOVERNMENT ENTERPRISE ARCHITECTURE
FOR INFORMATION COMMUNICATION AND TECHNOLOGY SERVICES
BUSINESS ARCHITECTURE
GOVERNMENT PLANS AND OBJECTIVES
GOVERNMENT METRIS
GOVERNMENT MONITORING (PERFORMANCE CONTRACTS)
APPLICATION ARCHITECTURE
PERSONAL IDENTIFICATION SYSTEM
CUSTOMER RELATIONSHIP MANAGEMENT
BUSINESS INTELLIGENCE
ELECTRONIC DOCUMENT MANAGEMENT
COMMUNICATION SYSTEM
FINANCIAL MANAGEMENT SYSTEMS
SECURITY SYSTEM
HUMAN RESOURCES MANAGEMENT SYSTEM
GEOGRAPHICAL INFORMATION SYSTEMS
MESSAGING AND COLLABORATIONS
PROJECT MANAGEMENT SYSTEM
PROCUREMENT MANAGEMENT SYSTEMS
PAYMENT GATEWAY
NATIONAL GATEWAY INFRASTRUCTURE
INFORMATION ARCHITECTURE
ANALYTICAL SERVICES
MASTER DATA MANAGEMENT SERVICES
ENTERPRISE INFORMATION INTEGRATION SERVICES (PROFILE, CLEANSE, ETL, FEDERATION, REPLICATION)
INFRASTRUCTURE ARCHITECTURE (SOFTWARE / HARDWARE LAYER)
LAN, WAN & INTERNET
COMPUTING
ENTERPRISE NETWORKS
STORAGE
DATA CENTRE
CHANNEL ARCHITECTURE
MOBILE
SERVICE PORTAL
CALL CENTRES
PROJECT MANAGEMENT AND GOVERNANCE
INTERGRATION ARCHITECTURE (SOA)
SECURITY AND COMPLIANCE
COUNTIES
GOVERNMENT AGENCIES PARASTATALS, INSTITUTIONS, COMMISSIONS
MINISTRIES
GOVERNMENT ENTRIES
ICT Authority

SOURCE: ICT AUTHORITY
LEVEL: 0 OF 3

Figure6: Government Enterprise Architecture

Architecture Principles

Architectural principles provide a set of general rules and overarching guidelines intended to support the long- term development and governance of the enterprise architecture. The goal of these principles is to apply constraints such that decisions reflect a balance of these elements, while providing maximum benefit to the organization. Principles are structured set of ideas that collectively define and guide the organization, from values through to actions and results providing a number of key benefits like -

Provide a framework within which the government can make conscious decisions around IT

Act as drivers for defining functional requirements for the architecture; and

Provide input for assessing the existing IT systems and developing future strategic portfolio

Enterprise Architecture Principle

The overarching vision for the EA is that it will be iterative and evolving, and will guide the development of an integrated information environment that will enable cost effective solutions to meet new business requirements. The intent of these basic generalizations is to ensure that the practice of architecture is holistic and continues to fulfil its intended purpose The Government enterprise architecture practice is mission-driven and aimed at promoting progress towards the goals of the Kenyan Government.

Enterprise Principles: Provide a basis for decision making throughout an enterprise, and inform how the organization sets about fulfilling its mission.

Business Architecture Principles

The Business Architecture principles are domain-specific principles built upon the foundation provided by the Government wide Enterprise Architecture principles. The intent of these basic generalizations is to guide the use and evolution of the Business Architecture methodology.

Information Architecture Principles

In general, the Information Architecture principles have been developed based on the premise that principles are formally defined statements of beliefs that enable decisions.

Information Architectures document the organization’s business and technology environment, and can include, but are not limited to, business services and processes, business locations, computer applications, databases, data marts, data warehouses, communications networks, access channels, data components and data services.

Application Architecture Principles

The application architecture principles provide the foundation for enterprise application development initiatives. It defines how applications should be designed to gain maximum interoperability for Ease of integration of applications, Efficient reuse of existing application assets, faster deployment of new applications, better responsiveness to changing business needs.

Technology Architecture Principles

Technology Architecture principles are described in this subsection grouped under the following major headings:

Technology Principles; and

Infrastructure Service Principles

These principles provide guidance for understanding how technology, services, patterns, blueprints, components, delivery levels, responsibilities, etc. Are required to develop, deliver, and manage technology. They also help determine the impact of potential changes to the technology architecture

Security Architecture Principles

This section presents security architecture principles grouped under the following categories:

- Administration;
- Availability;
- Accountability;
- Authorization;
- Assurance; and
- Awareness and Training

Integration Architecture Principles

This Identifies common components (including existing Government policies, standards, application, technology etc. wherever relevant) across the interoperability domain and define policies, standards, and procedures to ensure reusability of artefacts. There is need to have a perfect understanding of the MCAs IT solutions and prove to dive deeply into technology issues, in order to align Application solutions and IT Infrastructure.

This includes:

- Alignment & integration of the solutions defined in the IT strategy with cooperate strategy.
- Optimization of the technology capabilities of the information management platforms.
- Long-term life cycle responsibility for the MCA IT systems.
- Promotion of shared infrastructure and applications to reduce costs and improve information flows.
- Work with external solutions architect(s) to provide a consensus based enterprise solution that is scalable, adaptable and in synchronization with ever changing business needs.
- Management of the risks associated with information and IT assets in line with the enterprise security vision.
- Direct or indirect involvement in the development of policies, standards and guidelines that direct the selection, development, implementation and use of Information Technology within the enterprise.
- Project management and governance

Based on PRINCE2's seven principles which are that a project must:

- Have continued business justification (business justification principle)
- Learn from previous experience: lessons are sought, recorded and acted upon throughout the life of the project (learning from experience principle)
- Have defined and agreed roles and responsibilities within an organization structure that engages the business, user and supplier stakeholder interests (defined roles and responsibilities principle)
- Be planned, monitored and controlled on a stage-by-stage basis (manage by stages principle)
- Have defined tolerances for each project objective to establish limits of delegated authority (management by exception principle)
- Focus on the definition and delivery of products, in particular their quality requirements (focus on products principle)
- Be tailored to suit the project's environment, size, complexity, importance, capability and risk (tailoring principle).

COMPLIANCE, REVIEW AND EXCEPTIONS

MCA Enterprise Architecture

Sub domain	Requirement
EA development	Information Standards, policies and positions are developed using a defined process that includes: • pro-active identification of issues and risks associated with current and emerging business, service delivery, information management and ICT changes and issues • analysis to quantify the nature and scale of the issues being faced by government in order to identify the policy options available to address them • development of the most appropriate principles, policies, requirements and targets to achieve the desired results • consultation with impacted stakeholders, including review by specialist reference groups followed by general distribution to the affiliated MCAs and, in some cases, external stakeholders such as industry groups • submission to the appropriate governance bodies and approval authority • implementation of the policy, including undertaking business cases and resulting projects • evaluation of the principles, policies, requirements and targets through regular reviews, monitoring and annual reporting of compliance.

Key artifacts

Artefacttype	Focus	Description
Principle	What are the beliefs and values that will guide the Government to achieve its vision?	These represent the core beliefs and values of the GEA in relation to the management of information and underpinning technologies. They influence decisions made about the various resource and initiative portfolios across the sector and supporting processes.

Strategy	What general direction needs to be taken?	Strategies are short high-level documents intended to gain in-principle agreement from senior executives to a general course of action. The course of action will achieve an agreed desired future state or goal in support of the MCA's vision in the form of ambitions and priorities. To that end, strategies establish a baseline of the current environment; identify the drivers that are leading to the need for change to a particular environment; articulate the future desired environment; and propose a series of actions to realize that future desired state.
Standards / Policy	What are the specific directions, constraints and requirements which will achieve the MCA's strategies?	These artifacts are clear and specific statements of direction based on general principles which support achievement of long term strategies or provide a response to issues. They include detailed constraints and compliance requirements and in doing so they provide MCAs with an indication of the level of discretion available when making decisions. Information Standards and QGEA Policies are essentially equivalent.
Position	What targets must be met to realise the stated policy outcomes?	These provide detailed goal statements relating to either policies or requirements and the associated performance or objective measures that indicate realization of these goals.
Tools	How are the targets and policies to be met?	This isa general category for a range of supporting tools which assist MCAs and initiatives in the implementation of strategies, policies and positions. Virtually any useful information may be published in the EA as a tool. Common artifacts include definition papers, guidelines, templates, implementation advice and methodologies.

PRINCIPLES FOR THE GOVERNMENT ENTERPRISE ARCHITECTURE

a) GEA Foundation Principles

The GEA foundation principles intended to influence decision making to guide the formulation of policy. While articulated as independent principles, it should be recognised that there are synergies and potential overlaps between the principles.

Trustworthy: Information and information services are accurate, relevant, timely, available and secure

Rationale	Effective and valued government services can only be provided if they remain trusted by their users. It is essential that information used for the delivery of services is managed in an ethical and accountable manner throughout its lifecycle to ensure it is accurate, relevant, timely, available and secure.
Key implications	• Confidentiality, privacy, and security considerations must underlie all policy and investment decisions. • Reviews of information security environments must occur regularly. • Auditing mechanisms and procedures are in place to ensure appropriate confidentiality, privacy, security and access processes are maintained. • Integrity of information is vital to ensure it remains relevant and fit-for purpose (accurate). • Information must be maintained in a timely manner. Information which is out of date may be misleading and its ability to be trusted decreases the further out of date it becomes. • Maintaining high availability of information is critical to its ability to be used. MCAs should have appropriate business continuity plans in place to maintain the required availability of their information assets and relevant systems.

Transparent: Information must be routinely and proactively disclosed

Rationale	The Government is the custodian of significant amounts of public information. This information should be made readily available to the community to ensure government accountability and transparency and to allow the public to be more informed participants in the design and delivery of government services.
Key implications	• Right to information (freedom of information) considerations must underlie all policy and investment decisions. • Citizens should have access to and the ability to modify their own personal information provided to the government in line with the appropriate legislation. • Information collected at public expense is made available publicly wherever practicable, subject to privacy considerations • The collection of metadata about information, and its use to make information more discoverable must become part of the routine of government operations.

Leveraged: Share before Buy before Build

Rationale	Sharing and reuse of information and ICT assets and services, when widely practised, provides the basis for improved utility, value for money and performance. In order to maximise the value invested, investments must leverage existing initiatives and assets wherever practical.
Key implications	• 'Share before buy before build': • Sharing (including reuse) of assets is preferred to purchasing new systems or acquiring data independently. Systems should be acquired with the future need of sharing and reuse in mind. Systems which enable sharing and reuse should therefore be preferred over systems for which reuse or sharing will be difficult • sharing and reusing ICT and information assets and services to support government service delivery takes precedence over stand-alone and isolated systems • purchasing ICT solutions and services is preferred over building new systems • Building new systems, or implementing non-standard solutions, is only undertaken as a last resort when there is clear and demonstrable business benefits to an, as well as value for money returns to government. • Data collection is conducted on the basis of 'gather once, use many times'. • MCAs should be prepared to share their investments in software source code, architectures and other material with other MCAs.

Effective: Investments must be fit for purpose and deliver value and benefit

Rationale	Initiatives should only be undertaken if they have defined and measurable benefits. While self-evident, this principle has been included to explicitly reinforce the government's commitment to business outcome and benefit focussed investment.
Key implications	• Initiative approvals must be based on the delivery of measurable and meaningful service outcomes or other benefits. • Government services, and systems supporting the delivery of these services, should be designed, or re-designed, to operate in a way that is user-centred and intuitive to use and access and which facilitates rather than inhibits service delivery. • Systems and services should be regularly reviewed to ensure they continue to deliver the service outcomes and benefits intended. Those which are no longer achieving benefits should be decommissioned. • Information Management and ICT planning must be focussed on delivering business outcomes and benefits, and not be technology driven.

Aligned: Investments are aligned to priorities

Rationale	Alignment of business, information and ICT planning leads to improvements in performance, greater internal efficiencies and enables business priorities and Government business imperatives to be achieved more effectively.
Key implications	• Business priorities underpin IM and ICT planning and investment – information and ICT investments are based on business need. • Planned ICT solutions grow from business needs and are 'fit for purpose'. • Regular assessment of asset value and effectiveness in terms of business outcomes and service delivery is included as part of strategic planning and funding projections.

Equitable: Information services are accessible on an equitable basis

Rationale	Access to government services is important to maintain a fair society and strong economy. Therefore government information services are to be accessible in a manner that ensures social equity, regardless of geographic, economic or disability situations.
Key implications	• Arrangements exist to enable disadvantaged groups to access services as equitably as practical. • Equivalent fees are charged for access to equivalent information assets. • Government services have a consistent look and feel to meet the needs of all users and support equity of access by disadvantaged groups. • Government services are provided through multiple channels to suit the differing needs of disadvantaged groups.

Cohesive: The government is a single enterprise

Rationale	Given that Government is a single enterprise operating through many MCAs, the MCA and whole-of-Government business priorities need to be balanced to ensure effective and efficient service delivery. Innovation in government service delivery within an MCA should be promoted, as should opportunities to achieve better value from whole-of-Government approaches.
Key implications	• Whole-of-Government and MCA business priorities and considerations are balanced in all decisions. • The GEA and other whole-of-Government policy must guide whole-of-Government, cross-MCA and individual MCA investment decision making. • Investment decisions should support progression towards an integrated and consolidated service delivery i.eat a whole-of-Government level. • Opportunities are regularly sought for collaboration across MCAs for more efficient and effective government service delivery. Sharing the Existing ICT activities including ICT programs of work with ICTA provide a means for identifying such opportunities. Additionally, MCAs should consult with other relevant MCAs when developing programs of work and conducting MCA planning. • Information and system inter-operability considerations underlie information management practices and system selection and implementation. • Duplication and overlap of assets and services is minimised.

Managed: Services and assets are proactively planned and managed

Rationale	The IM and ICT services and assets of the Kenya Government represent a significant investment that underpins the continued delivery of services. These services and assets must be managed over time to ensure their operational performance is maintained and that ongoing service delivery risks are managed.
Key implications	• Comprehensive information management policies, procedures and practices must be defined and implemented to ensure that information is managed and maintained throughout its useful life. • Planning and investment arrangements for IM and ICT are formalised and apply agreed standards, methodologies and best practices. • Planning includes key stakeholders from business units. • Governance and management arrangements for IM and ICT are formalised. • Information custodianship underpins the management of information assets. • All change is managed, approved and executed according to agreed processes to minimise the risk of unforseen adverse impact on resources and services. • MCAs have formal architecture and policy functions to govern IM and ICT investments and assets. • Service continuity is managed, with business continuity and disaster recovery arrangements and capability maintained and tested regularly and comprehensively to ensure their ongoing effectiveness.

Compliant: Service and asset investments comply withlegislative and policy requirements

Rationale	ICT assets and services provided by MCAs on behalf of the Kenyan Government must comply with current legal, ethical, technical, economic, environmental and social responsibility requirements. Lack of compliance can lead to unforseen liabilities and litigation that could otherwise be avoided.
Key implications	• MCAs are accountable for the way they manage information and ICT services and assets. • Staff is educated and aware of compliance requirements in relation to the use of ICT services and assets. • Compliance requirements across MCAs are consistent, comprehensive, actively monitored and reported and regularly reviewed. • Compliance requirements are clearly documented, accessible and known across all MCAs.

b) Enterprise Architecture Principles (EAP)

PRINCIPLE	RATIONALE	IMPLICATION
EAP 1:The government focuses on citizens	• The government exists to serve the public who want simpler, faster, better and cheaper access to government services and information.	• Departments will design and apply their business processes and services to benefit citizens, even when the services cross lines of business. • The government offers citizens a single, unified face, reducing duplicate, needlessly complex, inconsistent ways of using government services. • Citizens can access government services through various means.
EAP 2:The government is a single, unified enterprise	• The government operates as a single enterprise with decision-making flexibility at the level. • A single enterprise with shared strategic objectives, common governance, integrated management processes and consistent policies improves the implementation of government-wide strategies and the coordination of the delivery of department citizen services.	• Government optimizes resource allocations across the enterprise to achieve common goals. • Government optimizes information across the enterprise to support services and processes. • Architectural designs integrate services for efficiency and keep autonomy of operations for effectiveness. • Architectural designs identify and accommodate distinctive (non-homogenous) approaches to maintain important policy objectives.

EAP 3:The Government architecture is mission-driven	• A business-led architecture is more successful in meeting strategic goals, responding to changing mission needs and serving citizens´expectations.	• Architecture is driven by program mission needs and enabling technology. • MCAs will first seek to optimize business processes, and then use performance standards to define automation requirements. • Systems and processes will use an architecture that responds quickly to events. • The government and MCAs will use their enterprise architectures to guide their capital planning, budget and investment decisions. • MCAs will manage change in government operations with enough security to keep services flowing. • Government solutions must be agile and flexible to meet business needs.
EAP 4: Security, privacy and protecting information are core government needs	• Security, privacy and protecting information are integral to government operations, and are part of the architecture. Government must protect information against unauthorized access, denial of service, and both intentional and accidental modification to increase public trust.	• The business context defines security and privacy requirements, which integrate into the entire architecture throughout the business lifecycle. • Architectures must reflect policies to minimize improper use of data and security violations. • Government must apply security and privacy consistently and monitor compliance. • Information security controls need to be clearly defined so cost and risk are balanced and managed.

EAP 5: Information is a national asset	• A well informed citizenry is necessary to our democracy. • Accurate information is critical to effective decision making, improved performance, and accurate reporting.	• The government will improve its information sharing environment to better disseminate information to the public. • This requires Government to identify authoritative sources of high quality information, and MCAs to provide access to specified data and information. • Authoritative data sources may need to be restructured and catalogued for easy dissemination, access and management. • To realize this principle requires a government strategy to promote cost effective data sharing with other levels of government.
EAP 6: The architecture simplifies government operations	• Architecture is designed to reduce complexity and enable integration to the maximum extent possible. • Complex processes and systems with tightly coupled modules are difficult to manage, risk failure, are inflexible to changing mission needs, and are expensive to maintain.	• This requires loosely coupled software components shared as services and compatible application development. • MCAs must share their best practices and reusable business and technical components. • Building and integrating reusable components must become a common development method. • Highly modular, loosely coupled systems and processes take advantage of shared services and reusable components within government and available commercially.

EAP 7:Enterprise Architecture is mission-driven	A business-led architecture is more successful in meeting strategic goals, responding to changing mission needs, and meeting citizens' expectations	• Ensure architectural descriptions demonstrate how the business serves the current • Government's priorities and the needs of citizens; • To the extent possible, design artifact type definitions to facilitate integration with descriptive representations of other jurisdictions, thereby allowing MCA to collaborate with each other.
EAP 8: Enterprise Architecture is aligned with relevant legal framework	• The Legal Framework, as contemplated in the Constitution, Acts and Regulations is designed by legislatures to ensure good governance, accountability, citizenship and an improved public service delivery in Kenya • Compliance to the legal framework reduces the risks of non-conformance and under-performance.	• Laws, regulations, and policies should be considered when developing Enterprise Architecture. • Changes in the law and regulations may drive changes in the Enterprise Architecture of departments and MCAs, in particular services, functions, processes and applications. • Business process improvements may lead to changes in the legal framework.
EAP 9: Simplification	An Enterprise Architecture that is explicit and pragmatic enables transformation of programs and services and minimizes enterprise redundancy.	• Optimize lines of business and business solutions to benefit the enterprise as a whole; • Maintain an EA practice designed to reduce complexity and enable integration to the maximum extent possible; • Make best practices available to ensure architectural representations from all five architecture domains provide a minimal set of information sufficient to describe fully problems, opportunities and solutions.

EAP 10: Reuse	Reuse minimizes development, complexity, maintenance and support costs through the deployment of common well-understood components	• Define architecture practices in each domain to produce and promote practical mechanisms for reuse; • Ensure reuse is one of the criteria of quality assurance review; • Encourage and reward reuse throughout the enterprise; and • Processes, applications and components are designed to meet reuse objectives
EAP 11:Explicitness	Explicit architecture facilitates creating and changing an enterprise and its business solutions. Formally developed and documented enterprise architectures form a baseline and provide an effective foundation for managing change.	• Define architecture practices in each domain to produce and promote pragmatic and useful artefact-type definitions; • Communicate best practices for artefact creation; • Grow and maintain an accessible collection of descriptive representations to provide an evolving picture of the enterprise.
EAP 12:Holistic	To provide business value over time enterprise architecture contains interrelated information covering all aspects of the enterprise at all levels of abstraction (business; information; application; technology; and security.	• Establish and mature the architecture practice in the five architecture disciplines; • Ensure artefact type definitions include the means by which transformation and • alignment are provable; • Ensure enterprise architecture review requirements include a set of artefacts from • each domain sufficient to contribute meaningfully to an enterprise view; and • Include transformation and alignment as criteria for architecture review.

EAP 13: Enterprise Architecture is aligned with relevant legal framework	Business architecture practice includes the discipline and tools required to enable business strategic and operational planning.	• Ensure business goals are aligned with enterprise priorities; • Position the business in the context of the broader enterprise; • Develop business model to meet operational objectives and strategic goals; and • Analyse business risk and develop strategies for risk management

c) Business Architecture Principles (BAP)

PRINCIPLE	RATIONALE	IMPLICATION
BAP 1: Business Planning	• Primacy of Principles • Service Orientation: Identify & Deliver Government Services that are Critical, Flexible & Reusable • Compliance with Legislation, Government Regulations and Standards	• Public service that is based on integrated approach to service that fosters coherence and compliance
BAP 2: Common vocabulary	A common business vocabulary enhances communication and understanding of the business	• Engage and consult with business stakeholders to ensure mutually agreeable business vocabulary; and • Ensure the business vocabulary is explicit.
BAP 3: Simple and Flexible	Opportunities for increasing efficiency, effectiveness, and quality can be identified and realized through simple and flexible business processes.	• Analyse business processes to simplify, integrate, eliminate redundancy, and increase efficiency; • Identify common business processes for reuse; and • Design business processes to enable business agility.
BAP 4: Technology independent	Business architecture describes the business model independently of supporting technology and provides the foundation for analysis of opportunities for automation.	• Eliminate technology constraints when defining business architecture; and • Ensure automated processes are described at the business process level for analysis and design.

BAP 5: Public and Private collaboration improves public services	Collaboration between public and private entities, who share government objectives, improves the efficient use of national resources; reduces duplication of effort and inconsistencies, and optimizes public service delivery.	• The BA structures and functions on IT Governance include governance functions (such as direct, evaluate and monitor) • The BA performance models include shared accountability on programmes as reflected in performance scorecards across public service departments and MCAs. • • The BA structures and functions includes partnerships across departments and MCAs, and among public and private sector. • The BA processes reflects that public service delivery processes traverse across traditional organisational boundaries. • System architecture reflects integration, interoperability and sharing of Information and ICT systems across all spheres of government to improve and optimise public service delivery. • Architecture reflects the adoption of open (non-proprietary) standards and industry's best practices.

BAP 6: Operations are optimised and simplified	Enterprise Architecture facilitates and enables business process effectiveness and efficiency and the reduction of complexity of systems to the maximum extent possible.	• Business processes and services are standardised in line with good practice and shared within and across departments. • Business processes are optimised and performance standards defined before automation requirements are defined. • • Systems and technology architectures are aligned with business processes and performance models in order to maximise the value of ICT investments. • Systems and software are modular, flexible and loosely coupled. • Information exchange interfaces are simple and based on open standards for all intra or interdepartmental solutions.

BAP 7: Systems are designed to ensure Business Continuity	Critical operations must continue in spite of system failure. System failures disrupt operations and lead to service delivery failures.	• Mission essential/critical systems are designed according to business continuity and disaster recovery requirements and include the necessary continuity measures (such as redundancy, standby and fail over components). • • Information Systems inventory is established and maintained and each system is classified commensurate their risk of failure profile (e.g. nonessential, essential, critical). • • Alternative business processes are followed only when recovery operations take place in the event of system failure. • • Essential/Critical systems use technology that is proven to be reliable and maintainable. • • Essential/critical systems are monitored and pre emptively reconfigured to ensure continued operations.
BAP 7: Service Orientation:	• identify & Deliver Government Services that are Critical, Flexible &Reusable • It is a key aim of any ICT vision to provide services in a flexible manner. This supports the target of improving service to citizens	• Reusing services across departments & ministries eliminate duplicity. Duplicative capability is expensive and contributes to the proliferation of conflicting data

d) Information/Data Architecture Principles (IAP)

PRINCIPLE	RATIONALE	IMPLICATION
IAP 1: Formally Defined and aligned with business needs	Well-defined information and data designs contribute to strategic decision- making processes and service delivery.	• Ensure the business information and data needs are clearly communicated; • Organize and document information holdings using information architecture processes, methods and standards; • Document the business information flows and linkages to enable a clear • Understanding by the data owners/custodians; • Model, design, and develop information holdings using a top-down, enterprise-wide architecture approach.
IAP 2:Information /Data security and permission	The duty to protect and secure sensitive information must be balanced against the duty to share and release public information. Laws and Regulations require the safeguarding of sensitive information while permitting free access to public information. In order for government to improve the security of its resources, it must protect its information from unauthorised access, modification or damage.	• Information System Security capability (people, processes and technology) is in place to determine, monitor and maintain the levels of security of the government information assets (data, applications and technology). • Security architecture is an integral part of business, data, application and technology architectures. • Security architecture is consistently applied throughout departments and systems. • Access control to information and data sources is applied within the data architecture (not in the application architecture).

IAP 3:Data is shared and duplication is reduced	• Data is a strategic resource that requires effective and efficient management across government. • Duplicate information and data sources across government systems result in duplicate labour intensive data management processes and frustrated citizens who need to provide same information to multiple departments. Duplication also • Leads to public service delivery inconsistency; fragmented data management responsibilities, reduced validity of data, poor data quality, and is open for localised exploitation and potential fraud and corruption.	• Business architecture (processes and functions) of information management includes the roles and responsibilities of "meta-data manager" (person who manages the design of data) and "data governor/steward" (person who manages data quality and integrity on behalf of someone else) as required for data sharing. • System architecture (data exchange and flow models) reflects intra and interdepartmental data exchange and verification models for inclusion in departmental transition plans. • Data sources that are candidates for re use and sharing across departments are determined in every architecture development project in order to reduce the burden of duplicate data collection (e.g. citizen data, geographic data, etc) and to improve the quality and validity of government data. • Shared data sources are consolidated into a shared environment to increase the re use and sharing. • On-line data exchange and verification interfaces across different data sources are standardised on best practice using data record exchange interfaces, in favour of bulk file transfers (such as large "flat-files" or "data dumps").

IAP4: Data is accessible	• Users – public servants and citizens alike – must have access to accurate, relevant and timely data to render or consume an effective government service. • A well informed citizenry is necessary to our constitutional democracy; and accurate information to authorised users is critical to effective decision making, improved performance, and accurate reporting.	• Government wide data catalogue (inventory) is developed and used to identify authoritative sources of high quality information that can be made available for access to empower public servant and citizens alike. • Default Access control to data is set to "open for all" and made available to all through any means, unless security policy requires access restrictions (i.e. application software should not unnecessarily restrict users to access data). • "Search" or "Find" functionality exist for all end-user applications/ web portals to improve access to data sources. • Access to data sources is available via various interfaces (access channels) to improve the convenience for the user.
IAP 5: Standard, Common vocabulary and data / metadata definitions.	• Data definitions that are consistent and meaningful ensure the effective and efficient development, interoperability and use of data and applications throughout government. • The power of a common vocabulary and data definition also enable effective dialogue to empower user and citizens.	• Government and MCAs should have common Dictionary of ICT Terms and Definitions on ICT that is freely shared and collectively owned by ICT practitioners. • A common data reference model (a schema that contains the data entities and their definitions), a meta data model (a schema that defines relationship between the data entities) and a meta data store (an electronic repository to store it) are well defined and available to whole of Government. • Develop clear information and data definitions to enable data sharing, integration, exchange and reuse across the enterprise;

IAP 6: Integrity, Accessibility And Availability	• Information needs to be concise and accurate (integrity), accessible, and available, as required by the business.	• Defines processes that provide for integrity, accessibility and availability of the information and data; • Ensure information owners and custodians are aware of the sensitivity of their information holdings they own/manage; and • Adhere to information architecture modeling standards, best practices, and guidelines.
IAP 7: Data has an owner/trustee		

e) Application Architecture Principles (AAP)

PRINCIPLE	RATIONALE	IMPLICATION
	• Modular and component based • Ease of use and re-use	
AAP 1: Common applications are shared across government	The sharing of applications that are designed to enable common/transversal business processes/ functions of government radically improves the economy of IT investments across government. Sharing of common/transversal applications reduces the burden of maintaining several configurations of the same type of applications, complexities in support contracts and commensurate licensing fees.	• Information system catalogue (inventory) is developed and used to identify candidates for common and transversal type applications. • Provision is made for MCAs to (1) dispose or modify some of their unique applications in favour of a common/transversal application standard, and (2) adapt existing business processes to align with the common/transversal business process. • Common/transversal applications use open interfaces to enable development of departmental specific extensions and to enable information exchange with departmental unique application portfolio. • MCAs retain data ownership to comply with legal or security requirements.

AAP 2: Applications are independent of technology infrastructure	• Applications that are independent from the underlying technology infrastructure allows applications to be designed, developed, operated on and migrated to a variety of front-office (end-user) and back-office (hosting environment) technology platforms to improve flexibility, end-user convenience, cost effectiveness and lower the risk of technology vendor lock-in.	• Application Development Software that does not support portability or platform independence is avoided. • Commercial Off the Shelf applications that are technology dependent are avoided. • Applications are designed for multi-tier deployment, which separates at least the end-user tier from the back-end tier, and the back-end tier from the database tier. • Traditional client-server applications that demands high-speed communications networks, high-performance end-user computers, or dedicated client (end-user computer) software, are not deployed over wide area networks.
AAP 3:Common applications are easy to use	Common applications (which are intended for broad deployment in government) that have consistent and simple user interfaces reduce the training burden and provide incentive for end-users to use the application.	• User interface design is informed by user location, language, competency, and physical capability. • Applications contain no unnecessary technical options that could reduce productivity and increase the risk of improper use of the application. • Same type applications have a common ''look-and-feel'', support ergonomic requirements and provide context sensitive help. • User friendliness is part of the test and acceptance criteria, which requires sign-off by an end-user representative, before applications are deployed for general use.

AAP 4: Traceability	• Aligns to business; • Build for change; • Facilitates transformation of business architecture; • Enhances traceability to business requirements; • Maximize the effectiveness of the development project; and • Minimizes requirement mismatch	• Need to ensure conformance to EA practice in the creation of artefacts; • Need to follow a Systems Development Life Cycle methodology or applicable standard; and • Need to document stakeholder requirements well

AAP 5: Flexibility	Application Architecture must be highly modular, multi-tiered, flexible, and loosely coupled. • Optimizes for agility; • Minimizes integration complexity; • Simplifies implementation, deployment and maintenance; • Enhances scalability, upgradeability, supportability; • Enables service and component reusability; • Ensures services are componentized; • Facilitates and improves maintainability; and • Enables technology platform changes with minimum effect on business processes; and • Enables Component-Based Architecture (CBA) & Services-Oriented Architecture (SOA)	• Need to implement n-tier architecture pattern; • Need to utilize application design patterns; • Need to establish a common approach to integration; • Must consider component- or services-based architectures; and • An enterprise Services-Oriented Architecture strategy may need to be in place

AAP 6: Integrability	Application Architecture must reduce integration complexity and foster application simplicity. • Reduces costs; • Streamlines business processes; • Facilitates reuse; • Improves integration; • Minimizes application impacts (e.g., potential delays in project completion); • Decreases application maintenance and support; • Minimizes duplication and multiple systems; and • Increases application flexibility	• Need to follow standards (industry, open-standard, technology, security, etc.); • Need to plan for integration; • Need to develop loosely-coupled interfaces; and • Need to publish integration points

AAP 7: **Modularity**	The Application Architecture must follow a service-based approach • Hides the complexity of heterogeneous IT environments from business user; • Allows internal and external business processes to be combined and recombined to support flexibility in business process execution; • Enhances business agility; • Provides an IT architecture that is more flexible, agile, and cost effective; • Helps to ensure better interoperability; • Supports services transformation; • Improves Service Offering; • Potential for cost reductions through IT asset re-use; • Creates opportunities for new business/services integration; • Better software and faster build (composite applications); and • Promotes collaboration	• Use standards-based approach; and • Security and privacy awareness heightened

AAP 8: Buy Versus Build	The Application Architecture must support the concept of reuse before buy and buy before build. • Reduces costs; • Aligns to business requirements; and • Minimizes application development, maintenance and support costs and related resource implications	• Need to conduct a fit/gap and cost-benefit analysis; • Need to comply with ICT directives and operating policies; • Need to be market-aware; • Need to plan for integration; and • Need to follow the acquired solution guidelines for conformance to EA practice
AAP 9: Consolidation	The Application Architecture must promote consolidation first and integration second. • Reduces cost; • Reduces integration complexity; • Facilitates consolidation of similar functions; • Streamlines similar application into single systems; • Minimizes duplication of solutions; • Increases reuse across the enterprise; and • Simplifies application maintenance and support	• Need to conduct a fit/gap and cost-benefit analysis; • Need to comply with ICT directive; • Need to plan for consolidation; and • Need to follow the acquired solution guidelines for conformance to EA practice

AAP 10: **Interoperability**	• Supports inter-jurisdictional initiatives; • Helps to view the government as a single enterprise; • Facilitates consolidation of similar functions; • Facilitates data sharing between internal and external partners; • Supports streamlining processes; and • Reduces cost	• Need for enforced security standards; • Require open or industry standards; and • Need to use standardized interface
AAP 11: **Reusability**	The Application Architecture must assist with designing applications for reuse. • Reduces cost; • Fosters enterprise reuse; • Encourages future reusability of its common components/services and applications; • Promotes application assembly and component integration; • Increases number of application/common components/services available for use by other new applications; and • Ensures consistency in the development of components/services	• Need to reuse existing application components or services where feasible; • Need to employ Component Based Architecture or Services-Oriented Architecture (SOA)as preferred architecture best practices; and • An enterprise Services-Oriented Architecture strategy may need to be in place

AAP 12: Share ability	The Application Architecture must take a portfolio approach to analyzing, planning, designing, governing, and optimizing enterprise applications. • Optimizes application investment; • Improvers reusability; • Improves application planning; and • Enhances IT asset management	• Reduces of the number of applications; • Focuses on application gaps; and • Enables an enterprise-wide application planning and prioritization approach
AAP 13: Upgradability	• The Application Architecture must anticipate and plan the replacement and transition of legacy applications. • Minimizes likelihood and risk of developing and deploying applications that are functionally deficient • Reduces likelihood of implementing solutions which are high-cost/ high- maintenance • Assists with planning for the replacement of applications - reduces 'crisis' • Replacement and maintenance efforts • Facilitates a responsive enterprise ICT posture that can respond to to changing requirements over time	• Need to establish a legacy renewal strategy • Both business and IT must work together in the search for the best possible replacement • Need to develop priorities for the replacement of obsolete, legacy and redundant • systems

AAP 14: Compliance	Application solutions must be developed using standard, common methodologies. • Standardizes development methodologies; • Increases likelihood of high quality deliverables; and • Reduces cost through common methodologies and tools	• Systems Development Life Cycle standards must be adopted to maximize the effectiveness of the development process; and • Training will be required to support standard methodologies
AAP 15: Supportability	The applications must be documented comprehensively to ensure that it: • Aligns to business; • Facilitates transformation of business architecture; • Enhances traceability to business requirements; • Maximizes the effectiveness of the development project; • Minimizes requirement mismatch potential; and • Supports future maintenance of the system	• Need to ensure adherence to EA practice in the creation of artifacts; • Need to ensure the application design reflects the application architecture principles, practices, and standards; • Need to ensure the requirements traceability by cross-referencing the system • requirements with design elements; and • Need to follow a development methodology and/or applicable standard

f) Technology Architecture Principles (TAP)

PRINCIPLE	RATIONALE	IMPLICATION
TAP 1: **Technological diversity is contained**	• Limiting the diversity of technology product mix on a government wide scale will reduce maintenance, supply chain complexities, and reduce the cost of procurement due to leveraging economy of scale; and technology innovation.	• The Technology product portfolio that is utilised for common/transversal systems is reduced to a finite manageable set that will strike a balance between the ease and cost of managing the life-cycle of technology on the one side, and stimulating healthy economic competition and growth of the ICT industry • The Technology product portfolio that is utilised for departmental unique systems is reduced to a finite set per department. This will allow each department to reduce the complexities per department, but also to have different technology portfolios from each other that will enable fair economic participation of the ICT industry. • Growing and evolving the ICT portfolio require that emerging, innovative or cutting-edge ICT products must be monitored on a continued basis; and be subjected to proof-of-concept to test for relevance, compliance and impact to government operations before it is introduced into ICT product portfolio. • The efficacy, efficiency and risk of the existing ICT product portfolio are reviewed on a regular basis to identify candidate products that need to be upgraded or disposed.

• TAP 2: Technology components are able to interoperate and exchange information	• Technology components (hardware and software), which cannot exchange information or integrate with each other lead to rampant duplication of data and ICT, and therefore introduces inconsistency and complexity in the ICT infrastructure portfolio.	• Government adopts interoperability standards whose specifications are freely available, non-proprietary, have multiple implementations and can easily be maintained; and publish such standards in a standards catalogue known as the Minimum Interoperability Standards (MIOS) for Government Information Systems). • A government-wide technology product catalogue must be developed and maintained to account for all the types of ICT products and to record their level of compliance with MIOS. • All prospective ICT products must comply with the MIOS before it is implemented in the Government ICT infrastructure; and all existing ICT products that do not conform to the MIOS must be part of a migration plan to become compliant with MIOS. • The MIOS is reviewed and updated on a regular basis to keep abreast with technological development through a process of research, consultation and consensus among government stakeholders.

g) Security Architecture Principles (SAP)

PRINCIPLE	RATIONALE	IMPLICATION
SAP 1: Administration – Protection of ICT Assets	• ICT assets and resources will be protected from loss, destruction or unauthorized use or disclosure in accordance with its value, sensitivity and applicable legal requirements. • The appropriate implementation of ICT security measures will be cost-effective and risk-appropriate investments.	• MCAs, ICT Clusters and service providers must effectively assess management and mitigate risks by defining, communicating, developing, improving and implementing.
SAP 2: Administration – Responsive and Cost-Effective	• The design and implementation of security infrastructure (e.g., identification, authentication and authorization services and mechanisms) will be as secure, pluralistic, simple, efficient, cost-effective, reusable and transparent to the end-user as possible. • The impact of security mechanisms and services on business productivity is minimized, encouraging compliance with the security policies and practices by way of a well-considered security model at the MCA, program and ICT Cluster level.	• Implement solutions in a manner that is consistent with the security tenet of limiting access based on end-user role (e.g., staff members, System Administrators, third party partners, commercial users and private/individual consumers of -offered services). • Develop and implement security mechanisms and ICT infrastructure that are neither intrusive nor invasive. • Develop and implement security mechanisms and ICT infrastructure that conform with government policies and standards regarding identity management, authentication and authorization , including: • Single system sign-on solutions; • Multi-factor authentication schemes; and • Authentication and authorization solutions based on smart-card and biometric approaches.

SAP 3: Administration – Auditable Compliance	• The security of ICT systems must be auditable, as required for compliance with statutory, contractual, and policy requirements as well as de facto security standards of care that may apply across jurisdictional boundaries. • Audit schedules for ICT systems are consistent with the security models and plans for technology solutions.	• Ensure ongoing security compliance and control; • Ensure security-appropriate standards of care are met regarding safeguarding of ICT assets • Ensure 3rd party service providers comply with GEAICT security policies, standards and requirements; and
SAP 4: Administration – Commensurate Controls	• All ICT systems will be designed, built and implemented to incorporate the level of assurance, security, privacy controls, auditability and control functions necessary and appropriate to the sensitivity and value of information assets and/or resources that they consume, control, utilize or manage.	The MCAs must define and communicate: • Security policies, standards and guidelines related to; Information and data sensitivity and classification; Criteria for determining appropriate level of assurance (Confidentiality, • Integrity, Availability) ; Authentication requirements; and Audit trail requirements • Security processes related to: Communications; Compliance; Security testing and evaluation (ST&E); Governance (review, endorsement and approval); and Audit (exceptions and appeals).

SAP 5: Availability – Security Process Support	• ICT enterprise security architecture addresses availability of information assets, ICT- based resources holding and supporting security infrastructure, processes and structures. • The enterprise security architecture will support key security processes such as monitoring and incident response, business continuity and contingency planning (business Impact/Risk Assessment and Analysis), disaster recovery, security configuration and capacity planning and security operations measures.	• The security standards and guidelines and operations processes must address: Monitoring and reporting; Incident response; Business continuity planning; Disaster recovery (DR) and contingency planning; Security design and implementation; Security configuration and capacity planning; Assurance; Forensics; and Security operations planning (e.g., identity and access control, user-id management).
SAP 6: Availability – Controls Consistent with Risk & Value	• Safeguards to protect against breaches of security will be implemented to reduce potential risk to ICT assets and resources. • The safeguards and level of response to threats will be consistent with the value, vulnerability and sensitivity of protected assets or resources.	• The ICT enterprise security architecture policies and procedures must include: • A statement defining what constitutes a breach of security and a delineation of which incidents and occurrences are security events rather than security incidents

SAP 7: Assurance – Standards-based Security Services	• The MCAs will adopt and comply with industry-accepted/standard approaches regarding due-diligence and standards of care in order to ensure the secure delivery of ICT- based services and seamless and incident-free information exchange. • Security measures will comply with GEA and industry standards and security will be upheld when parties interact either in a Government-to-Government (G2G), Government-to-Citizen (G2C), or Government-to-Business (G2B) context.	• ICT security architecture must define and improve: • Security processes and structures; • Communication strategies, materials, plans and resources; • Compliance-related information resources and training tools; • Asset control and protection strategies, services and mechanisms; • Monitoring and auditing protocols, processes and techniques; and • Enterprise-wide understanding of the legal ramifications for non-compliance with security-related policies, directives, and statutory/regulatory requirements.
SAP 8: Accountability – Ownership and Sensitivity Determination	• All ICT assets and resources must be accounted for and have an owner, steward and custodian identified, documented and designated. • The value and sensitivity of all ICT assets will be safeguarded in accordance with security directives, policies, standards and guidelines and the applicable statutory frameworks.	• Determine and assign responsibilities, accountabilities, obligation, conditions and rules for designating accountability and authority to parties for securing assets and resources; • Take inventory of all ICT assets and resources and designate person(s) accountable for same; • Design reasonable security measures and ensure they are implemented in order to safeguard the confidentiality, integrity and availability of ICT assets and resources; • Define a threat/risk mitigation process for design and development of enterprise-architecture and ICT systems and infrastructure;

SAP 9: Authorization – Auditable Rule-Based Access	• Access to information and information technology assets and systems must be controlled on the basis of business rules, conditions and obligations. • Access controls for operational systems must be demonstrably auditable	• Enable security, privacy and confidentiality by limiting access to information and ICT assets and resources in accordance with the principles of least privilege and separation of duties.
SAP 10: Authorization – Restricting Secure Facilities Access	• Access to secure locations will be restricted to those with legitimate requirements. • Security measures must isolate protected assets and resources from threats, consistent with the value and sensitivity of the information and data holdings. ICT assets must not be vulnerable to security threats or hazards.	• Ensure that standards are defined, approved, implemented, and enforced for safeguarding access to secure facilities and ICT assets.

SAP 11: Awareness and Training – All Government Employees Responsible	• Awareness of Information and IT security is the responsibility of every government employee and agent.Awareness and training facilitates the consistent execution of ICT security programs and plans across government and an adequate and uniform security posture for the organization.	• Include security and privacy responsibilities in job descriptions and contracts; • Train all employees and agents in security procedures and incident reporting processes; • Include compliance related wording in the conditions of employment as appropriate.

h) Integration Architect Principles

PRINCIPLE	RATIONALE	IMPLICATION
IAP 1: **Interoperability**	• Policies defined should reinforce & standards selected should facilitate interoperability • Identify common components (including existing Government policies, standards, application, technology etc. wherever relevant) across the interoperability domain and define policies, standards, and procedures to ensure reusability of artefacts. For e.g. defining data structure, data sets at a national level etc. Choose standards that will enable more choice and reduce the administrative burden.	• Eliminates patchwork of ICT solutions in different government offices those are unable to talk'or exchange data. Interoperability allows seamless exchange of information, reuse of data models and inter-changeability of data across systems • Brings in the ability to effectively interconnect, collaborate, access and facilitate data • Integration in order to communicate between different government organizations (G2G, G2C, and G2B etc.).

IAP 2: Confidentiality	• Guarantee the privacy of information with regard to citizens (e.g. health records), business (e.g. organization statistics) and government (e.g. confidentiality agreements) to help enforce the legally-defined restrictions on access & dissemination of information	• This will ensure that the confidential information and data are properly classified and adequately protected. • Privacy cannot be guaranteed by technical standards alone, it has to have process, inter-organisational agreements, cyber laws etc. in place to enforce it. • However fundamental tenet of this is to protect the integrity of government information and information held by various MCAs.
IAP 3: Open standards based	• Adherence to open standards should be promoted • Adoption of open standards will facilitate storing of electronic national records and data using open data file formats.	• Adherence to standard that will provide for choice of vendor will promote competitiveness and opportunity to look at cross platforms. The attributes of open standards such as platform independence, vendor neutrality and ability to use across multiple implementations and the model for establishing open standards are what • will allow for sustainable information exchange, interoperability, flexibility, data preservation & and greater freedom from technology and vendor lock-in

IAP 4: Enterprise Service Bus (ESB) based national service delivery gateway	• The use of ESB promotes loose coupling, support integration of heterogeneous systems, support adherence to open standards • ESB enables rapid development, assembly & deployment of services, ease ofmaintenance and improved business visibility	• The Enterprise Service Bus (ESB) should be the public API for the underlying implementation of the enterprise-wide Service Delivery Gateway. • There should be loose coupling between the service and its underlying layers with the service layer.
IAP 5: Web services for information exchange and granular service.	• By using web services to communicate between the service layers, the enterprise can create the ability to have a rationalized monitoring and security strategy for the Enterprise • Enable compliance with industry standard web service specifications of security, interoperability, reliability etc	• Web Services are to be used between the service layers. Granularity of the services composed in the ESB should not be too fine to promote a huge number of unmanageable services, where change in one, results in a cascaded set of changes in the others.

i) Project management and governance

PRINCIPLE	RATIONALE
Business justification	This means that it is not enough to assess the alignment to organizational objectives only when the project first starts; this should be done all the way through its life. To help, the PRINCE2 processes include activities to check for continued justification periodically
Learning from experience	Lessons are sought, recorded and acted upon throughout the life of the project
Defined roles and responsibilities	Have defined and agreed roles and responsibilities within an organization structure that engages the business, user and supplier stakeholder interests

Manage by stages	• Projects are planned, monitored and controlled on a stage-by-stage basis. • Breaking a project into a number of management stages provides senior management with control points at major intervals throughout the project. At the end of each stage, the project's status should be assessed, the Business Case and plans reviewed to ensure that the project remains viable, and a decision made as to whether to proceed. In essence it is a stop/ go type of review.
Management by exception	• The management by exception principle encompasses: • Delegating authority from one management level to the next by setting tolerances against the target objectives for the respective level of the plan • Setting up controls so that if those tolerances are forecast to be exceeded, they are immediately referred up to the next management layer for a decision on how to proceed • Putting an assurance mechanism in place so that each management layer can be confident that such controls are effective.
Focus on products	Focus on the definition and delivery of products, in particular their quality requirements
tailoring principle	Be tailored to suit the project's environment, size, complexity, importance, capability and risk

Table 1 – Compliance Checklist

DOMAIN	PRINCIPLE	REQUIREMENT	COMPLIANCE
Enterprise Architecture	EAP 1:The government focuses on citizens	Business processes designed and applied to focus on service to citizens provided as a single interface through multiple access platforms	
	The government is a single, unified enterprise	Government optimizes resource allocations across the enterprise to achieve common goals. Government optimizes information across the enterprise to support services and processes. Architectural designs integrate services for efficiency and keep autonomy of operations for effectiveness. Architectural designs identify and accommodate distinctive (non-homogenous) approaches to maintain important policy objectives.	
	The Government architecture is mission-driven	Architecture is driven by program mission needs and enabling technology. MCAs will first seek to optimize business processes, and then use performance standards to define automation requirements. Systems and processes will use an architecture that responds quickly to events. The government and MCAs will use their enterprise architectures to guide their capital planning, budget and investment decisions. MCAs will manage change in government operations with enough security to keep services flowing. Government solutions must be agile and flexible to meet business needs	
	Security, privacy and protecting information are core government needs.	The architecture must integrate policies and controls that ensures security, privacy, protection of information and minimise improper use of data throughout the business lifecycle. Government must apply security and privacy consistently and monitor compliance. Information security controls need to be clearly defined so cost and risk are balanced and managed.	
	Information is a national asset.	Information is an asset needed by citizens and leveraged across the government to improve performance	
	The architecture simplifies government operations.	This requires loosely coupled software components shared as services and compatible application development. MCAs must share their best practices and reusable business and technical components. Building and integrating reusable components must become a common development method. Highly modular, loosely coupled systems and processes take advantage of shared services and reusable components within government and available commercially.	
	Enterprise Architecture is mission-driven.	Ensure architectural descriptions demonstrate how the business serves the current Government's priorities and the needs of citizens; To the extent possible, design artefact type definitions to facilitate integration with descriptive representations of other jurisdictions, thereby allowing MCA to collaborate with each other.	
	Enterprise Architecture is aligned with relevant legal framework	Laws, regulations, and policies should be considered when developing Enterprise Architecture. Changes in the law and regulations may drive changes in the Enterprise Architecture of departments and MCAs, in particular services, functions, processes and applications. Business process improvements may lead to changes in the legal framework.	
	Simplification	Optimize lines of business and business solutions to benefit the enterprise as a whole; Maintain an EA practice designed to reduce complexity and enable integration to the maximum extent possible; Make best practices available to ensure architectural representations from all five architecture domains provide a minimal set of information sufficient to describe fully problems, opportunities and solutions.	
	Reuse	Define architecture practices in each domain to produce and promote practical mechanisms for reuse;	
	Explicitness	Define architecture practices in each domain to produce and promote pragmatic and useful artefact-type definitions; Communicate best practices for artefact creation; Grow and maintain an accessible collection of descriptive representations to provide an evolving picture of the enterprise.	
	Holistic	Establish and mature the architecture practice in the five architecture disciplines; Ensure enterprise architecture review requirements include a set of artefacts from each domain sufficient to contribute meaningfully to an enterprise view; and Include transformation and alignment as criteria for architecture review.	
	Enterprise Architecture is aligned with relevant legal framework	Ensure business goals are aligned with enterprise priorities;	

Business	PR-1: Strategic focus	Investment decisions are defined by business requirements	
	PR-2: Cohesiveness	MCAs shall present a consistent face of government through a common and consistent approach to service delivery.	
	PR-3: Reliability	Information and information services are reliable, accurate, relevant and timely	
	PR-4: Value	Government business initiatives and investments must represent value for money and return a business benefit	
	PR-5: Accessibility	Information and services are accessible on an equitable basis.	
	PR-6: Trustworthy	The integrity and confidentiality of information and data produced and managed by government is protected.	
Application	PR-7: Agility	Capabilities including business processes, information, applications, and technical assets are able to evolve and adapt to a changing environment.	
	PR-8: Quality	Capabilities including business processes, information, applications and technical assets meet quality service standards for performance, reliability, traceability and usability.	
	PR-9: Leverage	Reuse before buy. Buy before build.	
	PR-10: Harm minimisation	ICT systems, products and services are designed to meet sustainable requirements to minimise and manage their adverse environmental impacts.	
Information	PR-11: Asset	Data and information are assets that have value.	
	PR-12: Transparency	Information is accessible to the public, where appropriate.	
Technology Principles	PR -13: Ownership	All models, patterns, blueprints, components, services, and technologies shall have owners.	
	PR-14: Enterprise Technology Integration Model	Defines basic technology architecture concepts such as patterns, blueprints, components, services, quality levels, infrastructure catalogues and portfolios, etc., as well as the interrelationships between them.	
	PR -15: Quality Level Metric (QLM) Approach	Quality level metrics considered must be comprehensive and include all the categories and aspects. (scalability, availability, recoverability, security, integrity, user- bility, interoperability, etc)	
	PR -16: Infrastructure Maintenance	Infrastructure maintenance will be subject to SDLC rigour similar to that for a new application/technology deployment initiative.	
	PR -17: Rationalization of Products and Platforms	The variety of ICT products and platforms shall be rationalized. Technological diversity shall be controlled and minimized.	
	PR -18: Product Selection	Products shall be selected with regard to optimizing quality level metrics such as availability, technology standards, uniformity, the ability to integrate with existing systems, cost and comply with security and privacy requirements must be considered.	
	PR -19: Portfolio of Products	A portfolio approach should be adopted for planning and management of ICT of vendor supported ICT products, including software, hardware, and infrastructure	
	PR-20: Security/Privacy Design, Robustness and Resiliency	Security and Privacy must be designed into systems as an integral part of the technology design process. Systems shall be designed with robustness and resilience and so disaster recovery measures shall be put in place for all critical systems	
Infrastructure Service Principles	PR -21: Infrastructure	The design, implementation and delivery of infrastructure shall adhere to the technology architecture principles. The order of preference for infrastructure and infrastructure components will be to reuse, buy and then build. Use the current technology	
	PR-22: Service Development Life Cycle Framework	All ICT infrastructure services shall be defined and managed in accordance with a formal service development life cycle framework and process.	
	PR-23: Decomposition and Componentization of Services	All ICT infrastructure services, whether purchased or developed internally, shall be architected using the Service Decomposition Framework that identifies the IT component set, and IT components used to build the IT service.	
	PR-24: Portfolio of Infrastructure Services	A portfolio approach should be adopted for planning and management of ICT infrastructure services	
	PR-25: Infrastructure Service Quality Level Metric (QLM) Approach	Solutions, services, and infrastructure must be designed to optimize the quality level metrics. Quality level metrics considered must be meaningful, measurable and when required, enforced by SLA.	

Security Architecture Principles	PR-26: Administration – Protection of ICT Assets	ICT assets and resources will be protected from loss, destruction or unauthorized use or disclosure in accordance with its value, sensitivity and applicable legal requirements.	
	PR-26: Administration – Responsive and Cost-Effective	The design and implementation of security infrastructure (e.g., identification, authentication and authorization services and mechanisms) will be as secure, simple, efficient, cost-effective, reusable and transparent to the end-user as possible	
	PR-27: Administration – Auditable Compliance	The security of ICT systems must be auditable, as required for compliance with statutory, contractual, and policy requirements as well as de facto standards of care that may apply across jurisdictional boundaries.	
	PR-28: Administration – Commensurate Controls	All ICT systems will be designed, built and implemented to incorporate the level of assurance, security, privacy controls, auditability and control functions necessary and appropriate to the sensitivity and value of information assets and/or resources that they consume, control, utilize or manage.	
	PR-29: Administration – Conform to Policies & Standards	An ICT enterprise architecture will include a security architecture. The security architecture will conform to security policies, standards and guidelines as well as any related processes.	
	PR-30: Administration – Conform to Statutory Requirements	Compliance with standards and successor legislation is a mandatory requirement.	
	PR-31: Availability – Security Process Support	ICT enterprise security architecture addresses availability of information assets, ICT-based resources holding and supporting security infrastructure, processes and structures.	
	PR-32: Availability – Controls Consistent with Risk & Value	Safeguards to protect against breaches of security will be implemented to reduce potential risk to ICT assets and resources.	
	PR-33: Assurance – Standards-based Security Services	Adopt and comply with industry-accepted/standard approaches regarding due-diligence and standards of care in order to ensure the secure delivery of ICT- based services and seamless and incident-free information exchange.	
	PR-34: Assurance – Policy Compliance & Appropriate Response	As per Government directives and ICTA operating policies, Standards, procedures and guidelines, MCAs will comply with corporate policies and standards related to security as a minimum.	
	PR- 35: Assurance – Accountability for Risk Acceptance	ICT architecture or systems which do not comply with approved ICT Security Directives, Policies, Standards, Guidelines or Processes must be formally reviewed and risk accepted by both the Program Manager and Corporate Security Officer.	
	PR-36: Accountability – Ownership and Sensitivity Determination	All IT assets and resources must be accounted for and have an owner, steward and custodian identified, documented and designated.	
	PR-37: Accountability – Parties Adhere to Security Policies	Parties are accountable for the appropriate and responsible use of ICT assets and resources in support of the goals and objectives of the overall ICT enterprise security architecture.	
	PR-38: Authorization – Auditable Rule-Based Access	Access to information and information technology assets and systems must be controlled on the basis of business rules, conditions and obligations.	
	PR-39: Authorization – Restricting Secure Facilities Access	Access to secure locations will be restricted to those with legitimate requirements. Security measures must isolate protected assets and resources from threats, consistent with the value and sensitivity of the information and data holdings.	
	PR-40: Awareness and Training – All Employees Responsible	Awareness of Information and IT security is the responsibility of every employee and agent.	
	PR-41: Awareness and Training – Managers Responsible for Security Awareness and Training	Awareness and training programs are an integral and on-going component of the ICT security and it is the manager's responsibility to ensure staff members are adequately trained.	

Integration (SOA)	Interoperability		
	Confidentiality		
	Open standards based		
	Enterprise Service Bus (ESB) based national service delivery gateway		
	Web services for information exchange and granular service.		
Project management and governance	PR-13:		
	PR-14:	.	

Related Documents

Code Number:	Title
ICTA. 1.001: 2016	Government Enterprise Architecture
ICTA. 2.001: 2016	Infrastructure Standard (Networks, Cloud, End user Computing Device, Data Centre)
ICTA. 3.001: 2016	Information Security Standard
ICTA. 4.001: 2016	Electronic Records and Data Management Standard
ICTA. 5.001: 2016	IT Governance Standard
ICTA. 6.001: 2016	Systems and Application Standard
ICTA.7.001:2016	ICT Human Capacity Development Standard

ICT Authority
Telposta Towers, 12th Floor, Kenyatta Ave
P.O. Box 27150 - 00100 Nairobi, Kenya
t: + 254-020-2211960/62
Email: info@ict.go.ke or communications@ict.go.ke or standards@ict.go.ke
Visit: www.icta.go.ke
Become a fan: www.facebook.com/ICTAuthorityKE
Follow us on twitter: @ICTAuthorityKE

ICT Authority