THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE,
PUBLIC SERVICE MANAGEMENT

e-GOVERNMENT AGENCY

e-GOVERNMENT INFRASTRUCTURE ARCHITECTURE – STANDARDS AND TECHNICAL GUIDELINES

Document Number eGA/EXT/IRA/001

Issued by eGovernment Agency - November 2017

THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE,
PUBLIC SERVICE MANAGEMENT

e-GOVERNMENT AGENCY

Document Title

e-Government Infrastructure Architecture – Standards and Technical Guidelines

Document Number eGA/EXT/IRA/001

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Jabiri Bakari	Chief Executive Officer		

Table of Contents

1.0 OVERVIEW

1.1. Introduction

The e-Government Agency (eGA) is established under the Executive Agencies Act No.30, 1997, Cap. 245 as a semi-autonomous Institution under President's Office Public Service Management. eGA is charged with the mandate of providing coordination, oversight and provision of e-Government initiatives and enforcement of e-Government standards to Public Institutions. In executing its duties, eGA shall implement and maintain coordinated government operations for Information and Communication Technology (ICT) that include the formulation of standards and guidelines to effectuate the purposes of the Agency.

To realize the vision of e-Government in Tanzania and successfully implement eGovernment Strategy, it is of paramount importance that **"e-Government Standards and Guidelines"** are formulated. The e-Government Standards and Guidelines' aim is to assist in the delivery of more consistent and cohesive services to citizen and support the more cost effective delivery of ICT services by Government. A worldwide agreeable practice for conducting Government wide eGovernment analysis, design, planning and implementation, using a holistic approach at all times, for the successful development and execution of eGovernment Strategy is known as **"eGovernment Enterprise Architecture".** The e-Government Standards and Guidelines Structure is hereby designed to cover most requirements of eGovernment Enterprise Architecture. This means that eGovernment Enterprise Architecture is incorporated in "eGovernment Standards & Guidelines".

Management of e-Government Standards and Guidelines requires categorisation. There are **nine categories/areas** covering all aspects of eGovernment. The **seventh** area is **eGovernment Infrastructure Architecture**. The Infrastructure Architecture focuses on servers, workstations, storage and network infrastructure, software licensing, ICT vendor management, manpower and service support aspects of the Public Institutions. Design of infrastructure architecture adheres to the overarching technology infrastructure architecture principles (e.g. ICT infrastructure procedures, Quality of Service, ICT service delivery and support) and Service Platform, Storage and Infrastructure. The Infrastructure Architecture Standards and Technical Guidelines document has been derived from the *e-Government Enterprise Architecture as referred in e-Government Architecture Vision - Standards and Technical Guidelines (eGA/EXT/AVS/001).*

1.2. Rationale

Infrastructure Architecture aims to develop a structured, standardized, and consolidated set of infrastructure services that optimally support business processes and applications.

1.3. Purpose

In line with the above rationale, Infrastructure Architecture prevents overlapping and diversity of services, and thus reducing the complexity of managed services and life-cycle management. Moreover, with the standardization of infrastructure it allows Public Institutions to produces greater flexibility bottom-up, makes it easier to carry out expansions, changes and replacements in technology. Finally this will ensure that the defined Infrastructure Architecture Standards and Technical Guidelines are adopted across the Public Institutions.

1.4. Scope

This document applies to all Public Institutions and involved third parties (suppliers and contractors). The Public Institution Accounting Officer (Head of Institution), Head of ICT Departments, Application Developers, Security Officers, Application Architects, Network and Infrastructure Engineers shall be responsible for ensuring the effective implementation of these specific standards and technical guidelines associated with Infrastructure Architecture within their respective Institutions.

2.0 e-EGOVERNMENT INFRASTRUCTURE ARCHITECTURE

2.1. eGovernment Infrastructure Architecture Reference Framework

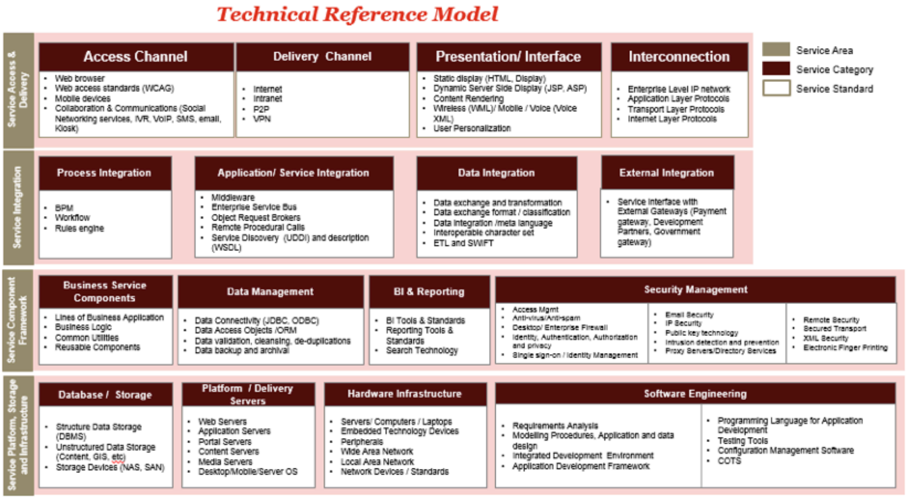
The Technical Reference Model (TRM) supports and enables the delivery of Application Reference Model service components and capabilities and provides a foundation to advance the re-use and standardization of technology and service components from a government-wide perspective. Aligning ICT capital investments to the TRM leverages a common, standardized vocabulary allowing cross departmental discovery, collaboration, and interoperability. Benefits from economies of scale will be obtained from identification and re-using the best solutions and technologies to support business functions, missions and target architecture. The TRM will continue to evolve with the emergence of new technologies and standards.

The TRM has been structured hierarchically as:

i. Service Area – Each Service Area aggregates the standards and technologies into a lower-level functional area. Each Service Area consists of multiple Service Categories and Service Standards.

ii. Service Category – Each Service Category classifies lower levels of technologies and standards with respect to the business or technology function they serve. In turn each Service Category is comprised of one or more service standards.

iii. Service Standards – They define the standards and technologies that support a Service Category. To support Public Institutions mapping into the TRM, many of the Service Standards provide illustrative specifications or technologies as examples. The proposed TRM for Government is depicted in Figure I:


Technical Reference Model

Service Access & Delivery

Access Channel
- Web browser
- Web access standards (WCAG)
- Mobile devices
- Collaboration & Communications (Social Networking services, IVR, VoIP, SMS, email, Kiosk)

Delivery Channel
- Internet
- Intranet
- P2P
- VPN

Presentation/ Interface
- Static display (HTML, Display)
- Dynamic Server Side Display (JSP, ASP)
- Content Rendering
- Wireless (WML)/ Mobile / Voice (Voice XML)
- User Personalization

Interconnection
- Enterprise Level IP network
- Application Layer Protocols
- Transport Layer Protocols
- Internet Layer Protocols

Service Integration

Process Integration
- BPM
- Workflow
- Rules engine

Application/ Service Integration
- Middleware
- Enterprise Service Bus
- Object Request Brokers
- Remote Procedural Calls
- Service Discovery (UDDI) and description (WSDL)

Data Integration
- Data exchange and transformation
- Data exchange format / classification
- Data integration /meta language
- Interoperable character set
- ETL and SWIFT

External Integration
- Service Interface with External Gateways (Payment gateway, Development Partners, Government gateway)

Service Component Framework

Business Service Components
- Lines of Business Application
- Business Logic
- Common Utilities
- Reusable Components

Data Management
- Data Connectivity (JDBC, ODBC)
- Data Access Objects /ORM
- Data validation, cleansing, de-duplications
- Data backup and archival

BI & Reporting
- BI Tools & Standards
- Reporting Tools & Standards
- Search Technology

Security Management
- Access Mgmt
- Anti-virus/Anti-spam
- Desktop/ Enterprise Firewall
- Identity, Authentication, Authorization and privacy
- Single sign-on / Identity Management
- Email Security
- IP Security
- Public key technology
- Intrusion detection and prevention
- Proxy Servers/Directory Services
- Remote Security
- Secured Transport
- XML Security
- Electronic Finger Printing

Service Platform, Storage and Infrastructure

Database / Storage
- Structure Data Storage (DBMS)
- Unstructured Data Storage (Content, GIS, etc)
- Storage Devices (NAS, SAN)

Platform / Delivery Servers
- Web Servers
- Application Servers
- Portal Servers
- Content Servers
- Media Servers
- Desktop/Mobile/Server OS

Hardware Infrastructure
- Servers/ Computers / Laptops
- Embedded Technology Devices
- Peripherals
- Wide Area Network
- Local Area Network
- Network Devices / Standards

Software Engineering
- Requirements Analysis
- Modelling Procedures, Application and data design
- Integrated Development Environment
- Application Development Framework
- Programming Language for Application Development
- Testing Tools
- Configuration Management Software
- COTS

Figure I: Technical Reference Model

Deriving from the TRM, the recommended Infrastructure Architecture Framework is depicted below.

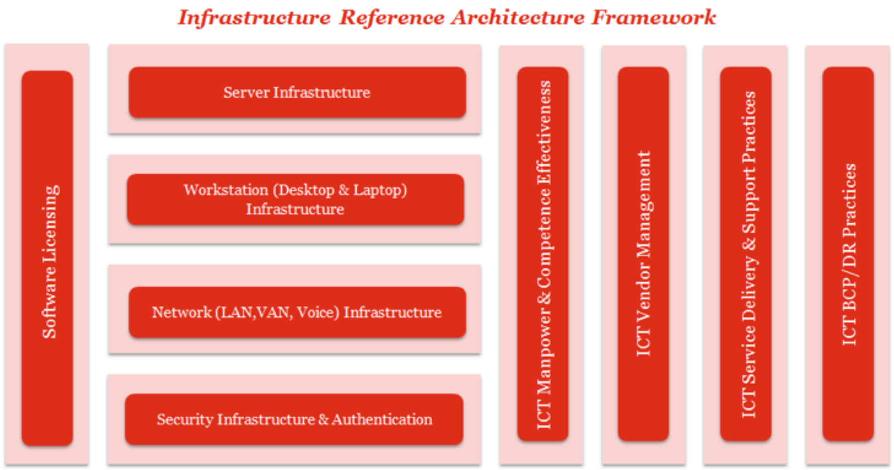

Infrastructure Reference Architecture Framework
Software Licensing
Server Infrastructure
Workstation (Desktop & Laptop) Infrastructure
Network (LAN,VAN, Voice) Infrastructure
Security Infrastructure & Authentication
ICT Manpower & Competence Effectiveness
ICT Vendor Management
ICT Service Delivery & Support Practices
ICT BCP/DR Practices

Figure I: Technical Reference Model

The Infrastructure Reference Architecture frameworks describes standards and guidelines for server, workstation, storage and network infrastructure, software licensing, ICT vendor management, manpower and service support aspects.

2.1.1 External Access, Exchange and Delivery of Service Components

For standards and specifications to support external access, exchange and delivery of Service Components or capabilities, Table I is the reference framework.

Table I: Standards and specifications to support external access, exchange and delivery of service components or capabilities

Service Type	Service Component	Service Component Capabilities
Access Channels	i. Web browser ii. Web access standards (WCAG) iii. Mobile devices iv. Collaboration and communications v. Telephony	i. An access channel defines the interface between an application and its users, whether it is a browser, smart phone, tablet or other medium. ii. Web browser – Examples of web browsers includes Microsoft Internet Explorer

		(IE), Mozilla, Firefox, and Google Chrome. iii. Web access standards – Examples includes WCAG by W3C (web accessibility guidelines), ISO 9241-151:2008 Guidance on World Wide Web user interfaces, etc. iv. Mobile devices – Examples include smart phones and tablets etc. v. Collaboration and communications – Examples includes social networking, Short Message Service (SMS), Interactive Voice Response (IVR), Voice over Internet Protocol (VoIP), Kiosks, Emails etc.
Delivery Channels	i. Internet ii. Intranet iii. Virtual Private Network	i. VPN – The use of public telecommunication infrastructure to connect Public Institutions and entities together, maintaining privacy through the use of a tunnelling protocol and security procedures. ii. The Internet standards as defined by the Internet Engineering Task Force (IETF).
Interconnection	i. Enterprise Level IP Network ii. Application Layer Protocols iii. Transport Layer Protocols iv. Internet Layer Protocols	i. Enterprise Level IP Network such as IPv6. ii. Application layer protocols such as DNS, DHCP, FTP/FTPS, HTTP/HTTPS, IMAP, IRC, LDAP, MIME, SNMP, POP3, RIP, SMTP, SOAP, SSH, Telnet etc.

		iii. Transport layer protocols such as TCP, UDP, DCCP, ECN. iv. Internet layer protocols

2.1.2. Interfacing with Service Components

During interfacing both internally and externally with a service component, Table II is the reference framework.

Table II: Internally and externally interfacing with service component standards.

Service Type	Service Component	Service Component Capabilities
Process Intergration	i. BPM ii. Workflow engine iii. Rule engine	i. Business Process Notation (BPMN) 2.0, Business Process Execution Language (BPEL), Business Activity Monitoring (BAM)
Application / Service	i. Enterprise Application Integration Middleware ii. Enterprise Service Bus iii. Object Request Brokers iv. Remote Procedural Calls v. Service Discovery and Description	i. Message oriented middleware – (IBMMQ, MSMQ, JMS, JMX, for Monitor and Optimise ii. ORB – CORBA , COM, DCOM iii. Service Discovery –UDDI iv. Service Description – WDSL, API
Data Intergration	i. Data exchange and transformation ii. Data exchange format and classification iii. Data integration meta language iv. Interoperable character set v. Extract, transform and load	i. Character encoding for information interchange – ASCII, Unicode, UTF-8 ii. Data description – RDF, XML, XNAL, XCIL, XCRL iii. Data exchange and transformation – XMI, XSLT, ISO 8601 for data element and interchange format iv. Data exchange formats – UN/EDIFACT, EDI, XML/EDI,

		XLINK, PDF, doc, ppt, xls, tiff, jpeg,rtf, MPEG, PST, CSV, HTM, AVI/MP3/ MP4 v. Ontology-based information exchange – OWL vi. Data integration meta language – XML vii. Signature and encryption – XML, DSS, XML , Key management specifications SAML, XACML viii. Data Types / Validation – DTD, XML Schema ix. Data Transformation - XLST
External Intergration	i. Service interface with external gateways (payment mechanisms, external agency, government gateway)	i. Banking integration – SWIFT ii. Tanzania Inter-bank Settlement System - TISS

2.1.3. Distributed or Service-Orientated Architectures Service Components

For specifications by which Service Components are built, exchanged, and deployed across Distributed or Service-Orientated Architectures Table III is the reference framework.

Table III: Distributed or Service-Orientated Architectures Service Components Standards

Service Type	Service Component	Service Component Capabilities
Presentation/ User Interface	i. Static Display ii. Dynamic / Server-Side Display iii. Content Rendering iv. Wireless / Mobile / Voice v. User Personalization	i. Static Display - Examples include HTML, PDF ii. Dynamic / Server-Side Display - Examples include JSP, ASP, ASP.Net iii. Content Rendering - Examples include DHTML, XHTML, CSS, X3D

		iv. Wireless / Mobile / Voice -WML, XHTMLMP, Voice XML v. User Personalization
Business Service Component	i. Lines of Business Application Business Logic ii. Web Services iii. Common Utilities iv. Reusable Components	i. Application business logic: ii. Platform Independent -EJB, C++, JavaScript iii. Platform Dependent -VB,VB. NET, C#, VB Script
Data Management	i. Database Connectivity ii. Data Access Objects/ORM iii. Data Validation, Cleansing / De-duplication iv. Data Backup and Archival	i. Data exchange -XMI, XQuery, SOAP, ebXML, RDF, WSUI ii. Database Connectivity - DBC, ODBC, ADO, OLE/ DB, DAO, DB2 Connector
BI and Reporting	i. BI Tools and Standards ii. Reporting Tools and Standards iii. Search Technology	i. Reporting and Analysis - OLAP, XBRL, JOI.AP, XML for analysis
Security Management	i. Access Management ii. Anti-Spam / Anti-Virus iii. Desktop and Enterprise Firewall iv. Identity, Authentication, authorization and privacy v. Single-Sign On / Identity Management	i. Access management - Support for OS, App server, DBMS, IDM and directory service standards, password encryption during storage and transmission ii. Digital Signatures - Secure hash algorithms, authentication, message integrity, non repudiation iii. Email Security - S/MIMEv3 iv. Encryption Algorithm - DES, triple DES

	vi. Email Security vii. IP Security viii. Public Key Technology ix. Intrusion Detection and Prevention x. Proxy Servers / Directory Services xi. Remote Security xii. Secured Transport xiii. XML Security xiv. Electronic Finger Printing	v. Enterprise Firewall - Support various layers of TCP/IP protocol stack, support for OS, network protocols, data transport, electronic mail systems and app technologies standards vi. Identity , Authentication , authorization and privacy - SAMLv1.1,X.509 for identity certificates, vii. Identity management - Support for OS, App server, DBMS, IDM and directory service standards, password encryption standards for storage and transmission viii. IP security - IPSec ix. Proxy server -Compatible with LDAPv3, able to integrate with adopted standards for directory services x. Remote Security - SSH xi. Secure transport -TLS/SSL xii. XML security standards -WS-Security, WS-1 Basic Security Profile Version, XML-DSIG

2.1.4. Delivery and Support Platforms

For specifications relating to delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component or capabilities, Table IV is the reference framework.

Table IV: Delivery and support platforms, infrastructure capabilities and hardware requirements.

Service Type	Service Component	Service Component Capabilities
Database/ Storage	i. Structured Data Storage ii. Unstructured Data Storage iii. Storage Devices	i. Structured data storage (DBMS) - DBMS should provide support for basic properties of a database transaction - atomicity, consistency, isolation, durability, support for data security, built-in audit, JDBC, ODBC, web service standards, transactional and analytical data should be in separate data store e.g. DB2, Oracle, SQL Server, Postgress SQL, Sybase ii. Unstructured data storage - Content server, GIS server iii. Storage devices -NAS, SAN
Platform and Delivery Servers	i. Web Servers ii. Application Servers iii. Portal Servers iv. Content Servers v. Media Servers vi. Desktop OS vii. Mobile OS viii. Server OS	i. Wireless / Mobile -J2me ii. Platform Independent -JEE, Linux, Eclipse iii. Platform Dependent - Windows, .NET, Mac OS iv. Web Servers -Apache, IIS v. Media Servers -Windows media service vi. Application Servers -Weblogic, Websphere, JBoss, iLOG, Oracle business rules, Jrules vii. Portal Servers - Liferay, JBoss portal, Oracle web centre viii. Content Server -Alfresco,

		ix. Desktop OS -Windows, Mac x. Server OS - Windows Server 2003/2008, Unix, Linux, xi. Mobile OS -Android, iOS, Blackberry
Hardware Infrastructure	i. Servers / Computers ii. Embedded Technology Devices iii. Peripherals iv. Wide Area Network v. Local Area Network vi. Network Devices / Standards	i. Servers / Computers - Enterprise server, mainframe ii. Embedded Technology Devices - RAM, RAID, microprocessor iii. Peripherals - Printer, scanner, fax, cameras iv. Wide Area Network (WAN) - Frame Relay, DSL, Metro Ethernet, ATM v. Local Area Network (LAN) - Ethernet, VLAN vi. Network Devices / Standards - Hub, switch, router, gateway, NIC, ISDN, Ti/T3, DSL, firewall
Software Engineering	i. Modelling process, application and data design ii. Integrated Development Environment iii. Application Development Framework iv. Programming language for Application Development v. Testing Tools vi. Configuration Management Software	i. Modelling process, application and data design - BPMN for process modelling, BPEI4WS for web services, ERD for data modelling, UML 2 and above for app modelling, XML schema v1.o, WML V2.0 ii. Integrated Development Environment - RAD, Visual Studio, Eclipse, Net beans, JDeveloper iii. Application Development Framework - Use of enterprise framework for app development, support for reuse of existing components and services, provide support for creating web services

	vii. Commercial Off The Shelf (COTS) Software	iv. Programming language for Application Development - Language should allow for code portability, code collaboration, browser compatibility, should be compatible with the app development framework adopted v. Testing Tools -Tools to be selected for functional testing, usability testing, performance, load and stress testing, security testing, reliability testing, regression testing vi. Configuration Management Software -version control, defect tracking, issue tracking, change management, release management, requirement management and traceability vii. COTS Software - applications should support open standards and other industry standards that promote interoperability with other products/ vendors, access to training, allow parameterization and customization for local needs

2.2. eGovernment Infrastructure Architecture Standards

2.2.1. Table V provides principle under which the eGovernment Infrastructure Architecture is designed. Institutional infrastructure architecture component of enterprise architectures should also be designed basing on this principle (There is an example in the Appendix).

Table V: Infrastructure Architecture Design Principle

Principle	Infrastructure resilience and scalability
Rationale	i. Resilience entails availability, archival and backup. ii. Scalability is required to support the overall SLA requirements. This involves scalability, availability & performance issues.
Implications	i. **Scalability:** Technology standards chosen will meet the changing and growing Public Institution needs and requirements and the applications and technologies will essentially scale up, to adapt and respond to such requirement changes and demand fluctuations. Server, storage and network capacities must handle user, application and data loads. ii. **Availability:** The technology infrastructure will exhibit no single point of failure. iii. **Archival and Backup:** The infrastructure will have data and source spanning across multi years. The archival and backup policy and mechanism will address the archival and backup requirement of the system and be aligned with the regulatory requirements. iv. The system infrastructure will be architected considering failover requirements and ensure, a single server or network link failure does not bring down the entire system (although e.g. performance may degrade). v. The system will handle every request and yield a response and handle error and exception conditions effectively. vi. In the event of failures or crashes, recovery of transactions and data will be possible. vii. The platform solution will support effective disaster recovery. viii. Monitoring of systems health at regular intervals will be possible. Use of central system, monitoring tool would be required to gauge the health of the system all time and monitor against the pre-defined SLA.

2.2.2. The following are standards for server infrastructure:

i. Server Infrastructure has to be used to store Public Institutions data and provide crucial ICT Services to end users.

ii. Select well known hardware manufacturers/vendors that provide relevant technical support, warranty on hardware failures and are continually ensuring that equipment is tested for full compatibility with well-known operating systems.

iii. Implement server management software tools that can assist with management and troubleshooting of server hardware and software. The outcome is a reduced cost of server infrastructure deployment and associated downtime.

2.2.3. Implement a centralized management of authentication, group policy management and patch management.

2.2.4. Ensure that all workstations on the network have the fundamental tools for self-protection, including: personal firewall, anti-spyware/malware protection, disk-based data encryption, basic security reporting.

2.2.5. In terms of network infrastructure and connectivity, ensure that high quality, reliable, scalable and measurable network connectivity is available at all sites. Mission critical sites have to be engineered for fault tolerance. This implies that in mission critical sites such as Server Rooms or Computer Rooms networks will be configured to ensure no single point of failure.

2.2.6. Ensure that the network is planned for and provides Quality of Service (QoS) to support the on-going convergence of Voice over IP (VoIP), data and wireless technology.

2.2.7. Maintain accurate and up to date network topology diagrams and documentation. Primarily, the documentation is required for network issue isolation and troubleshooting. Additionally, when preparing for growth, infrastructure upgrades, or architectural redesign requires a comprehensive understanding of the current network topology.

2.2.8. Make use of sound design principles, open standards and long range planning for core network services such as the Directory Services, Domain Name Services (DNS) and IP addressing (using Dynamic Host Configuration Protocol (DHCP) in a structured manner. These require careful consideration not only during the network design but also during physical implementation.

These services will enforce the ICT policy, facilitate access and securing of the ICT resources on the network and provide audit logs for reconstructing events etc.

2.2.9. Shift towards pooling the storage infrastructure as the servers themselves are consolidated. By making use of Storage Area Networks (SANs) and Network Attached Storage (NAS) technologies over the current Direct Attached Storage Devices (DASD) currently in Use and coupled with a more centralized backup platform there will be:

i. Greater utilization of storage

ii. Improved backup and restoration of data Easier storage administration

iii. Lower cost per megabyte

iv. Greater consistency in stewardship

2.2.10. For security infrastructure and authentication standards refer to *eGovernment Security Architecture - Standards and Technical Guidelines (eGA/EXT/ISA/001)* for additional details.

2.2.11. Public Institutions should have knowledgeable and appropriately skilled human resources accountable for its on-going ICT operations, management, maintenance, maturity and evolution. Appendix – *Illustration No. 1 ICT Organisation Capability* provides the generic list of required ICT capabilities in a Public Institution.

2.2.12. An achievement of high quality infrastructure services depends on the establishment of appropriate service level targets with service providers and holding the providers accountable to these targets.

a) Make sure that every vendor provides a Service Level Agreement (SLA) and measurement tools are established to ensure SLAs can be monitored.

b) Ensure that vendors have the capability to measure and report network performance (Local as well as wide-area / Internet / etc.) In the case of network management systems,

2.2.13. A vendor escalation process should be in place to escalate issues that are not resolved by the vendor in a timely manner as committed.

2.2.14. Maintain vendor performance records to support decision making whilst renewing or terminating vendor contracts. Vendor and Service provider performance metrics include but not limited to:

a) Deliveries and Responsibilities
b) Timing of Service
c) Quality of Service and Products
d) Repair or maintenance and Warranty

2.3. eGovernment Infrastructure Architecture Technical Guidelines

2.3.1. With respect to Server Infrastructure, run the latest version of the server operating system. In addition to providing additional features and functionality, latest versions will improve overall security of the server's data and services.

2.3.2. Opt for open source or commercial alternatives when necessary as choices for Centralized management of authentication, group policy management and patch management.

2.3.3. Implement Information and Application Access Anywhere. This can be done by deploying role-based configurations. Virtual Machines (VMs) can be used for users, independent of hardware and OS. VMs provide seamless migration for mobile computing, enable personalized applications and computing environments anywhere and provide shared server-based computing for task workers with centrally stored data.

2.3.4. Consider lowering the cost of ownership and improve reliability by moving towards standardization of both the hardware employed as well as software desktop image (consisting of the operating system, and suite of commonly used applications). This standardization, coupled with the greater use of management tools (such as Microsoft System Management Server, Dell KACE, LANDESK ad other) will greatly improve reliability, reduce downtime and risk.

2.3.5. While periodic replacement of the workstation population will allow for better total cost of ownership, mass wholesale replacement the entire workstation population will result in undesirable cost of ownership metrics. It is recommended that abide by best practices which dictates that 1/4 to 1/3 of the workstation population should be replace periodically so as to reduce overall maintenance cost and by extension the cost of ownership.

2.3.6. Consider replacing older PCs with new ones provide the benefit of improve operating system, improve security and improve speed and by extension improved productivity.

2.3.7. Consider remote support for workstations to increase productivity. This will facilitate implementation of software changes enterprise-wide, creating centralized desktop configuration database and monitoring drift from compliant, baseline configuration, and enabling enterprise-wide remote access, diagnosis, and repair.

2.3.8. Network Planning - The success of any infrastructure is measured in terms of how well the infrastructure planning choices match with the objectives of the functions of the Institution. Better networks require less maintenance consider upfront investments in planning, which will give assurance for smoother-running environment later on.

2.3.9. Ensure a properly deployed environment which will facilitate each of the following key network management functions: Network Discovery Process, Network Topology Visualization, Availability Management, Incident Management, ICT Asset Management, Configuration Management, Performance Management, and Problem Management. *Creation of ICT Service Management Procedures - Technical Guide (eGA/EXT/BSA/003).*

2.3.10. Public Institutions should adopt Information Technology Infrastructure Library (ITIL) which is a set of concepts and policies for managing ICT infrastructure, technology, development and operations. ITIL gives a detailed description of a number of important ICT practices with comprehensive checklists, tasks and procedures that any Public Institution can tailor to its needs.

2.3.11. Application Response Times – networks will provide application response times acceptable to support business needs and cost effective bandwidth to satisfy current and future networking needs of employees, citizens, external agencies and other users.

2.3.12. Track software inventory, versions, and physical placement. There are PC, Mac and LAN inventory packages which can be implemented by Public Institutions to control licensed software and will also do an audit of the software on a desktop/ server machines / LAN. Monitoring and tracking software licensing and compliance ensures that the software management processes are working effectively and that unlicensed / illegal software applications are not being used. In addition to this, tracking what software is used and how often it is used will assist Public Institutions to monitor licensing compliance and promote sharing and optimum utilization of licensed software. It is recommended that Public Institutions make use of widely available tools for tracking and recording workstation inventory.

2.3.13. Implement active directory restrictions to prevent the installation of unauthorized software. Introducing copied and unlicensed software into the computing environment can open the computer systems up to the risk of damage to your network through defective software or malicious code.

2.3.14. Public Institutions should migrate towards new technologies such as Microsoft Windows 8 and above since it offers ICT administrators an increased control over user activities.

2.3.15. Consider monitoring and reviewing of supplier services to ensure that all terms and conditions of the agreements are being adhered to and that issues and problems arising in the event of non-compliance are managed properly.

2.3.16. Adopt a formalised ICT asset disposal and reuse process in accordance to regulatory requirements to achieve the following:

i. Gain maximum value from the equipment through compliant and safe reuse, redeployment and disposal options.

ii. Ensure the complete destruction of data or hardware under maximum security.

2.3.17. Adopt enterprise licensing models for their application portfolio and leverage on Government licensing agreements to reduce total cost of ownership. Only suitably licensed software may be used in all Public Institutions.

2.3.18. Public Institutions will ensure compliancy to their Acceptable ICT Usage Policy in line with their ICT Policy.

2.3.19. Public Institutions shall adhere to the procurement processes for the acquisition, development and maintenance of all ICT equipment and software in line with institutional ICT Policy and ICT acquisition procedures.

2.3.20. Public Institutions will develop their **ICT Acquisition, Development and Maintenance Procedures** as guided by *"Creation of ICT Acquisition, Development and Maintenance Procedure - Technical Guide (eGA/EXT/IRA/003)* document.

2.3.21. For managing ICT infrastructure, technology, development and operations adhere to Institutional ICT Acquisition, Development and Maintenance Procedures.

2.3.22. Public Institutions will develop their Institutional **ICT Service Management Procedures** as guided by *"Creation of ICT Service Management Procedures – Technical Guide (eGA/EXT/IRA/002)"* document.

2.3.23. To develop ICT Service Management Procedures, as guided by *"Creation of ICT Service Management Procedures – Technical Guide (eGA/EXT/IRA/002)")"* document, Public Institutions should consider developing ICT service support and delivery within the organisation to ensure that the ICT end user can fully leverage on the technological platform. The services that may be considered include but is not limited to:

i. ICT asset management – to have an inventory of all ICT assets and to manage the life cycle of the ICT assets.

ii. Incident management - to restore Public Institutions normal service as quickly as possible, and to minimize the adverse impact on business operations.

iii. Service request management - to enable ICT users to request and receive standard services within a predefine time frame.

iv. Helpdesk management – to provide a standardize framework for registering and resolving reported ICT issues.

v. Change management - to ensure that standardized methods are used for the efficient and prompt handling of all changes, changes are recorded in a Configuration Management System and that overall business risk is optimized.

vi. Problem management - to prevent problems and resulting incidents from happening, to eliminate recurring incidents and to minimize the impact of incidents that cannot be prevented.

vii. Capacity management - to provide a point of focus and management for all capacity and performance-related issues, relating to both services and resources, and to match the capacity of ICT to the agreed business demands

viii. Configuration management – to ensure that all hardware and software are configured in line to leading practices and appropriately hardened.

ix. Availability management – to ensure that the ICT systems meet the availability requirements of the Public Institutions through the adoption of appropriate disaster recovery mechanisms.

x. Release management - to ensure that Public Institutions include the appropriate checks and controls prior to include new hardware or software within the production environment.

xi. IT service continuity management – to have the appropriate redundancies in place in terms of resources in view to provide a round the clock service to the Public Institutions.

xii. Service catalogue and service management – to assist the ICT team in selecting the ICT services that would be operated based on the business needs and the technical capabilities of the ICT team.

2.3.24. Public Institutions shall leverage on existing whole of Government e-Government initiatives such as Government Network (GOVNET), Government Mailing Systems (GMS), Government Data Centre (GDC) and Government Mobile Platforms.

2.3.25. The Government's aim is to have an electronic register of ICT equipment:

i. In the transition period each Public Institution must have an ICT equipment registry as shown on the Appendix A of the *Public Service circular No 5, 2009.* Therefore, Government institutions are required to hold correct information of their ICT equipment.

2.3.26. Public Institutions will consider the following general requirements with regards to the use of mobile data storage:

i. The Correct Use of Mobile Data Storage Device

a. Public servants should be educated regarding the safe use of ICT before commence using the devices.

b. Public servants must use the mobile data storage devices only on Government work. However, it is not permitted to mix official information and private information in the same device.

c. Public documents on transit via flash disk, portable hard drives, phones, iPOD etc. must be deleted from these devices once the transfer process is completed.

d. Public servants must not use CD ROM, DVD, and back up tapes for unintentional transfer or storage of information for future uses.

e. Public offices when procure mobile data storage devices must adhere to the directives from the President's Office, Public Service Management.

ii. Registration of Mobile Data Storage Devices

a. Mobile Data storage devices should be registered in institution's ICT asset registry with the user information as directed by Public Service circular No 5 of the year 2009.
b. Transfer of mobile data storage devices must adhere to the regulations guiding the issuing of office equipment.

iii. Storage/Sage Keeping of Mobile Data Storage

a. Mobile data storage devices must be stored in the Government Offices by the Government's guides for safe keeping of information and equipment. If a public servant requires to take the storage devices outside the Government Office he/she must inform the authorised person.

b. When the mobile data storage device is lost, the loss must be reported to the authority immediately for necessary actions to be taken.

iv. Destruction/Decommissioning of Mobile Data Storage Devices
a. When the use of mobile data storage device (when the device becomes obsolete), the device must be sent to the Directorate of Records and Archives Management (DRAM) for destruction.

b. It is forbidden to sell, issue as a gift, or to switch the ownership of Government's mobile data storage devices.

2.3.27. Public Institutions will comply with *Government Data Centers Guidelines and Procedures (eGA/EXT/IRA/002)* while using Data Center services provided by eGA.

2.3.28. Further references (Templates and Technical Guides) related to e-Government Infrastructure Architecture will be developed from time to time

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

3.1 This document takes effect once approved in its first page.

3.2 This document is subject to review at least once every three years.

3.3 Any exceptions to compliance with this document should be approved in writing by Chief Executive Officer (CEO) of e-Government Agency.

4. GLOSSARY AND ACRONYMS

4.1 Glossary

None

4.2 Acronyms

Abbreviation	**Explanation**
BCP	Business Continuity Planning
DAS	Data Acquisition System
DASD	Direct Attached Storage Devices
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Services
DR	Disaster Recovery
DRP	Disaster Recovery Planning
ICT	Information and Communication Technology
NAS	Network Attached Storage
QoS	Quality of Service
SAN	Storage Area Network
SLA	Service Level Agreement

SSH	Secure Shell
SSL	Secure Socket Layer
TRM	Technical Reference Model
VLAN	Virtual Local Area Network
WAN	Wide Area Network

5. RELATED DOCUMENTS

5.1. eGovernment Guideline 2016 by President's Office – Public Service Management (PO-PSM)

5.2. eGovernment Architecture Vision - Standards and Technical Guidelines (eGA/EXT/AVS/001)

5.3. eGovernment Interoperability Framework - Standards and Technical Guidelines (eGA/EXT/GIF/001)

5.4. eGovernment Business Architecture - Standards and Technical Guidelines (eGA/EXT/BSA/001)

5.5. eGovernment Application Architecture - Standards and Technical Guidelines (eGA/EXT/APA/001)

5.6. eGovernment Information Architecture - Standards and Technical Guidelines (eGA/EXT/IFA/001)

5.7. eGovernment Integration Architecture - Standards and Technical Guidelines (eGA/EXT/ITA/001)

5.8. eGovernment Security Architecture - Standards and Technical Guidelines (eGA/EXT/ISA/001)

5.9. eGovernment Architecture Processes and Governance - Standards and Technical Guidelines (eGA/EXT/PAG/001)

6. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	eGA	Creation of Document	February 2016
Ver. 1.1	eGA	Alignment with eGovernment Guideline 2016	November 2017

APPENDIX

Illustration No.1 ICT Organisation Capability

Table AI is a generic list of ICT organizational capabilities required for any Public Institution:

Table AI: ICT organizational capabilities required for any Public Institution

ICT Organisation Capability	Description
ICT Strategy and Planning	Capability to execute ICT strategy, Enterprise architecture (technical, application, and process), and budgeting/resource e planning.
IT Governance	Ability to develop and execute value management, performance management, project management, and ICT policy/procedures.
Risk Management	The ability to develop and execute proper security, ICT continuity planning, and compliance with legislation or standards
Applications Management	The capability to execute on application development, procurement, maintenance, quality, and data management.
Service Management	Includes the ability to develop and execute proper service planning, monitoring, delivery, and support for networks, storage, applications, etc.
IT Resource Management	Includes the ability to develop and execute on talent management, vendor management, outsourcer management, and ICT knowledge management.
ICT Infrastructure Management	Include ability to design, deploy, operate and manage the ICT Infrastructure efficiently and effectively, it includes the overall Server, Storage, Network and Security Infrastructure explicitly.

Illustration No.2 Typical Infrastructure Architecture

The diagram in Figure AI illustrates a typical infrastructure architecture that will be prepared by Public Institution by taking into consideration Client Layer, Presentation Layer, Integration Layer, Business Logic Layer, Enterprise Information System Tier/ Data Tier.

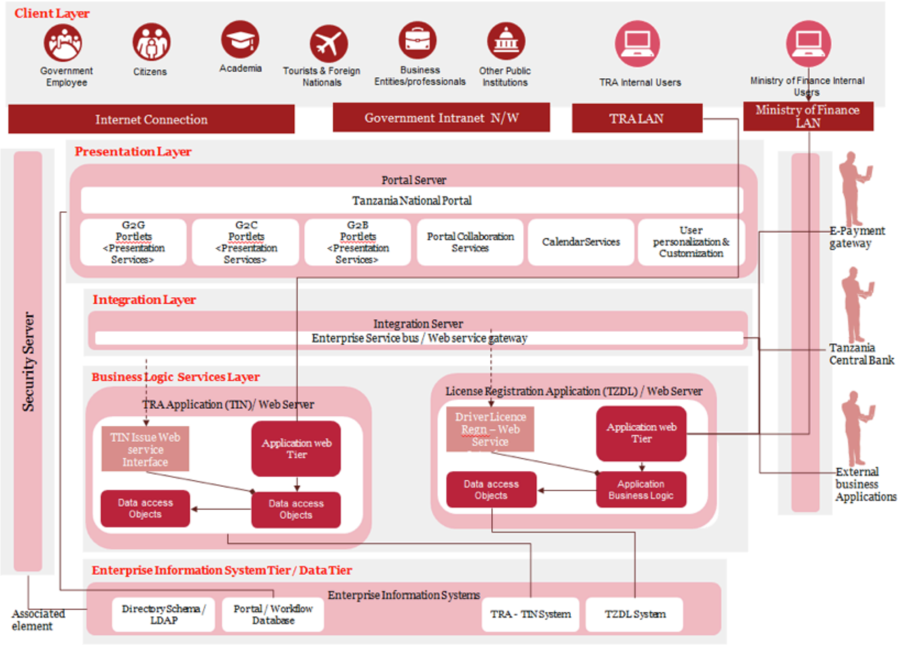

Client Layer
Government Employee
Citizens
Academia
Tourists & Foreign Nationals
Business Entities/professionals
Other Public Institutions
TRA Internal Users
Ministry of Finance Internal Users
Internet Connection
Government Intranet N/W
TRA LAN
Ministry of Finance LAN
Security Server
Presentation Layer
Portal Server
Tanzania National Portal
G2G Portlets <Presentation Services>
G2C Portlets <Presentation Services>
G2B Portlets <Presentation Services>
Portal Collaboration Services
Calendar Services
User personalization & Customization
Integration Layer
Integration Server
Enterprise Service bus / Web service gateway
Business Logic Services Layer
TRA Application (TIN)/ Web Server
TIN Issue Web service Interface
Application web Tier
Data access Objects
Data access Objects
License Registration Application (TZDL) / Web Server
Driver Licence Regn – Web Service
Application web Tier
Data access Objects
Application Business Logic
E-Payment gateway
Tanzania Central Bank
External business Applications
Enterprise Information System Tier / Data Tier
Enterprise Information Systems
Directory Schema / LDAP
Portal / Workflow Database
TRA - TIN System
TZDL System
Associated element

Figure AI: Typical Infrastructure Architecture

Issued by eGovernment Agency - November 2017