THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE, PUBLIC SERVICE MANAGEMENT AND GOOD GOVERNANCE

e-GOVERNMENT AUTHORITY

ISO 9001:2015 Certified

Document Title

Quality Assurance Compliance Guidelines for e-Government Applications

Document Number

eGA/EXT/APA/007

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Eng. Benedict B. Ndomba	Director General		14/05/2024

PREFACE

Since the world is moving into the era of automation, mobile apps, and post-pandemic life, reliance on software and applications continues to increase. Building quality software means solving existing problems without creating new problems that can be done through a proper Application Quality Assurance Testing.

Software quality assurance (SQA) is a process which assures that all software engineering processes, methods, activities and work items are monitored and comply against the defined standards such as Standards for e-Government Application Architecture Standards and Technical Guidelines, Development, Acquisition, Operations and Maintenance of e-Government Applications and etc., developed by the e-Government Authority. SQA incorporates all software development processes starting from defining requirements to coding until release.

The Quality Assurance Compliance Guidelines was intended to ensure e-Government applications developed by Public Institutions adhere to development practices that promote quality solutions.

Therefore, The Authority call upon all public institutions to comply with these quality assurance compliance guidelines for e-Government applications in order to ensure the intended benefits are achieved.

Eng. Benedict B. Ndomba
DIRECTOR GENERAL

Table of Contents

PREFACE **1**
1. INTRODUCTION **3**

1.1. Overview 3
1.2. Purpose 3
1.3. Rationale 3
1.4. Scope 3

2. THE COMPLIANCE GUIDELINES **4**

2.1. Applications Quality Requirements 4
2.2. e-Government Applications Compliance Guidelines 4
2.3. e-Government Application Quality Compliance Reviews 5

3. IMPLEMENTATION, ENFORCEMENT AND REVIEW **5**
4. GLOSSARY AND ACRONYMS **5**

4.1. Glossary 6
4.2. Acronyms 6

5. RELATED DOCUMENTS **6**
6. DOCUMENT CONTROL **6**
APPENDICES **7**

APPENDIX A: CHECKLIST FOR ACQUISITION AND DEVELOPMENT OF e-GOVERNMENT APPLICATIONS 8
APPENDIX B: CHECKLIST FOR OPERATION AND MAINTENANCEOF e-GOVERNMENT APPLICATIONS 11

1. INTRODUCTION

1.1. Overview

e-Government Authority also known as "e-GA" is a Government institution which was established on September 2019 under the e-Government Act No. 10 of 2019. The Authority is mandated to coordinate, oversee and promote e-Government initiatives and enforce e-Government related policies, laws, regulations, standards and guidelines in Public Institutions.

This document establishes guidelines to auditors/assessors during verification of adherence of e-Government applications to quality requirements in line with section 5(2) (a) and 22(2) of e-Government Act No.10 of 2019.

1.2. Purpose

Quality Assurance Compliance guidelines aims at enabling Public Institutions to review quality of their applications, auditors to assess compliance to quality assurance requirements as well as assist quality assurance officers assist management in understanding the quality status of their applications.

1.3. Rationale

Public Institutions have been implementing e-Government applications that sometimes fail to achieve the desired objectives or fail to meet evolving requirement of Institution and their users. In light of this, the Government requires a professional way of ensuring that acquisition, development, operation and maintenance is done according to quality requirements. This document will aid in ensuring that those operations are in compliance with quality assurance requirements.

1.4. Scope

This document will be applicable to all Public Institutions undertaking acquisition, development, operation and maintenance of e-Government Applications.

2. THE COMPLIANCE GUIDELINES

2.1. Applications Quality Requirements

2.1.1. Public Institutions should comply with quality requirements described in e-Government Application Architecture *(eGA/EXT/APA/001)*, particularly the ones available in the following standards and guidelines;

i. Standards for Development, Acquisition, Operations and Maintenance of e-Government Applications *(eGA/EXT/APA/005);* and

ii. Guidelines for Acquisition, Development, Operations and Maintenance of e-Government Applications *(eGA/EXT/APA/006)*

2.1.2. Public Institutions should comply with Government directives on applications whenever they are issued.

2.2. e-Government Applications Compliance Guidelines

These guidelines shall be used for self-assessment by Public Institutions or for independent assessments by auditors or quality assessors. The knowledge of application acquisition, development, operations and maintenance is a prerequisite in using this compliance guide. Therefore, during application acquisition or development the assessor or auditor shall:

2.2.1. Check on YES column against each criterion for the application that meets quality requirements on **All Checklists in the Appendices;**

2.2.2. Provide remarks on the checked N/A or NO columns;

2.2.3. Provide recommendations that will assist Public Institution improve the quality of the acquired/developed application; and

2.2.4. Produce quality assurance report with the following sub-headings;

i. Executive summary;

ii. Scope i.e., assed Institution and applications;

iii. Findings; and

iv. Recommendations.

2.3. e-Government Application Quality Compliance Reviews

2.3.1. A public institution by itself or using a qualified third party shall perform a self-quality compliance review;

(i) Before putting any e-government application into operation and copy of the reports should be submitted to e-Government Authority;

(ii) Annually for applications which are in operations and copy of reports be submitted to e-Government Authority;

(iii) At any stage of application acquisition, development, operations or maintenance as may be decided by the institution for its own control; and

(iv) By assessing each application separately; however, reports may be combined and attached with each application checklists.

2.3.2. A public institution shall report explicitly any non-compliance to quality compliance requirements as identified during assessments, accompanying with reasons and evidence if any; and

2.3.3. Verification of reports will be done randomly with regard to Government requirements by CAG, IAG, e-GA or any other independent Public Institution(s).

3. IMPLEMENTATION, ENFORCEMENT AND REVIEW

This document shall be:

3.1. Effective upon being reviewed by e-GA Management and signed by the Director General on its first page;

3.2. Subjected to review at least once every three years or whenever necessary changes are needed; and

3.3. Consistently complied with, any exceptions to its application must duly be authorized by the Director General.

4. GLOSSARY AND ACRONYMS

4.1. Glossary

Term	Description
Application	A Is a program or a group of programs designed for end users i.e., software and application software designed and developed/acquired for the Government of Tanzania in order to serve citizens better.

4.2. Acronyms

CAG	Controller and Auditor General
DRP	Disaster Recovery Plan
e-GA	e-Government Authority
IAG	Internal Auditor General

5. RELATED DOCUMENTS

i. e-Government Guidelines ***(PO-PSM, 2017)***
ii. e-Government Application Architecture – Standards and Technical Guidelines ***(eGA/EXT/APA/001)***
iii. Standards for Development, Acquisition, Operation and Maintenance of e-Government Applications ***(eGA/EXT/APA/005)***
iv. Guidelines for Development, Acquisition, Operation and Maintenance of e-Government Applications ***(eGA/EXT/APA/006)***

6. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	Quality Assurance Compliance	Creation of the document	November 2018

	Guidelines for e-Government Applications		
Ver. 1.1	Quality Assurance Compliance Guidelines for e-Government Applications	Inclusion of platform independence (checklist No 1.8 & 2.2 on APPENDIX A)	August 2019
Ver. 1.2	Quality Assurance Compliance Guidelines for e-Government Applications	Aligning the document with e-Government Act No. 10 of 2019., eGA/EXT/APA/005 Ver 2.0 and eGA/EXT/APA/006 Ver 2.0	May 2024

APPENDICES

APPENDIX A: CHECKLIST FOR ACQUISITION AND DEVELOPMENT OF e-GOVERNMENT APPLICATIONS

1. General Consideration for Application Development and Acquisition					
Question		**Yes**	**No**	**N/A**	**Remarks**
1.1.	Does the internal ICT team have appropriate knowledge and skills?				
1.2.	Does the application address business requirements?				
1.3.	Did the requirements originate from user department?				
1.4.	Does the requirement include security requirements?				
1.5.	Are the risks appropriately managed?				
1.6.	Was the internal ICT team involved?				
1.7.	Was it planned in Institution Strategic Plan/ICT strategy/ICT Policy?				
1.8.	Is the application developed/acquired capable of using different databases and operating systems i.e. platform independent?				
1.9.	Is the necessary IT infrastructure available to support the application from the Institution or Government?				
1.10.	If it is an application acquisition /development project, has it been reviewed by e-GA?				
1.11.	Is knowledge transfer part of application acquisition /development?				
1.12.	Was the requirement gathered reviewed and SRS produced?				
1.13.	Was the requirement document signed off by user department?				
1.14.	Was User Acceptance Test performed and signed by user department?				
1.15.	Do Project changes follow the institutional ICT project change management procedures?				
2. Application Acquisition					
Question		**Yes**	**No**	**N/A**	**Remarks**
2.1.	Does the acquired application from vendor necessitated by the lack of internal capacity and failure to get				

	assistance from other public institutions?				
2.2.	Is the acquired application platform independent?				
2.3.	If it is a common business support application, has e-GA been consulted?				
2.4.	Does the licensing scheme meet user department needs?				
2.5.	Does the institution have the capacity to manage application acquisition project?				
2.6.	Did the application acquisition follow Government procurement procedures?				
2.7.	Are the trainings related to the application provided/planned?				
2.8.	Has the contract negotiation been done by knowledgeable/relevant staff?				
2.9.	Are roles and responsibilities of both parties (Public Institutions and vendor) stated clearly?				
2.10.	If the application is institutional specific, does the institution own the source code?				
2.11.	Was there an extensive testing on test environment before deployment of application?				
3. Application Development					
Question		**Yes**	**No**	**N/A**	**Remarks**
3.1.	Does the Institution internal ICT team possess necessary knowledge and skills to develop the application?				
3.2.	If the internal ICT team lacks the requisite knowledge and skills to develop the application, does the institution seek assistance from other public institutions instead of vendor/freelancer?				
3.3.	If it is a large/complex application, was it developed in phases?				
3.4.	Did each phase produce a verifiable deliverable?				
3.5.	Was every phase properly documented including testing?				
3.6.	Has the application been developed with the most recent version of the framework for the chosen technology?				

3.7.	Do all application codes include sufficient comments for support personnel?				
3.8.	Are the mechanisms for tracking errors/bugs in place?				
3.9.	Did the application use approved institution/government software development methodology?				

APPENDIX B: CHECKLIST FOR OPERATION AND MAINTENANCEOF e-GOVERNMENT APPLICATIONS

1. General Checklist for Application Operations and Maintenance					
	Question	**Yes**	**No**	**N/A**	**Remarks**
1.1.	Does the institution have the ICT Service Support Desk?				
2. Internal Operations					
	Question	**Yes**	**No**	**N/A**	**Remarks**
2.1.	Are the applications hosted in the institutional approved equipment room or Government Data Center?				
2.2.	Is there a backup plan?				
2.3.	Is the backup taken as per plan?				
2.4.	Is the backup tested and results documented?				
2.5.	Is there a DRP ?				
2.6.	Is the DRP been tested and results documented?				
2.7.	Does the internal ICT team have the requisite knowledge and skills to support the application?				
2.8.	Has the application been handed over to operations department?				
2.9.	Has it been assigned application administrator(s)?				
2.10.	It there OLA with Institution user departments?				
2.11.	Is OLA compliance satisfactory?				
2.12.	Are privileged operations, events and incidents logged and auditable by Institution?				
2.13.	Are application logs audited regularly (i.e. monthly or less)?				
2.14.	Is ICT security handled internally?				
2.15.	Has the application been tested for security in less than 12 months ago?				
2.16.	Was there no security improvement required?				
2.17.	Has the application security improvement been made?				
2.18.	Has the application passed the required application testing requirements?				

2.19.	Does the application meet user and operation requirements?				
2.20.	Are there no bugs/errors hindering Institution operations?				
2.21.	Does the application produce logs which are stored for the agreed/required period?				
2.22.	Are all application operations guided by documented process, procedures and guidelines?	s			
2.23.	Are procedural operations such as adding users documented/captured for future references?				
3. Internal Maintenance					
Question		**Yes**	**No**	**N/A**	**Remarks**
3.1.	Has the business process been re-engineered/changed?				
3.2.	Is the change management process and procedures available and documented?				
3.3.	Has the maintenance need been raised through formal requests or through existing plans?				
3.4.	For procured applications, has the vendor released upgrade/patch/fixes and they are available for incorporation at no additional cost?				
3.5.	Is change management process being adhered to during application maintenance?				
3.6.	Has the changes, improvement, fixes been documented?				
3.7.	Do the tests done (application tests, security tests and related) after maintenance show that the application maintenance was successful?				
3.8.	Has the user department been satisfied with the maintenance done?				
4. Outsourced/Vendor Maintenance					
Question		**Yes**	**No**	**N/A**	**Remarks**
4.1.	Is there a license/contract for maintenance and still valid?				
4.2.	Is support/upgrades part of existing license/contract?				
4.3.	Does the vendor release upgrade/patch/fixes that are				

	available for incorporation at no additional cost?				
4.4.	Does the vendor disclose what is new/ changed before upgrading/ patching your application?				
4.5.	Is there a room for testing or evidence of testing for the changed/maintained application?				
4.6.	Does the maintained application function as required?				