Challenges of Using Open Source Applications in Government.  
  
1. Lack of Technical Expertise.  
In both Tanzania Mainland and Zanzibar, many government institutions have struggled to implement or sustain open source solutions due to a shortage of skilled ICT professionals.  
  
For instance:  
  
The Zanzibar e-Government Agency (eGAZ) and the e-Government Authority (eGA) on the mainland aim to promote open source and digital systems. However, in their own assessments, they have reported capacity challenges—including a shortage of software developers, cybersecurity experts, and open source system administrators.  
  
Reference   
United Republic of Tanzania. ([2020](tel:2020)). National ICT Policy Implementation Framework ([2020](tel:2020)–[2025](tel:2025)). Ministry of Communications and Information Technology. Retrieved from <https://www.mtc.go.tz>/  
  
e-Government Agency (eGA). ([2018](tel:2018)). Strategic Plan [2018](tel:2018)–[2023](tel:2023). Retrieved from <https://www.ega.go.tz>/

2. Resistance to Change  
  
Government employees are often used to proprietary software like Microsoft Office, and they may resist migrating to open source alternatives such as LibreOffice or Linux-based systems. This resistance is fueled by lack of awareness, fear of change, or discomfort with new systems.  
  
Reference:  
Chigona, W., & Licker, P. S. ([2008](tel:2008)). Using diffusion of innovations framework to explain communal computing facilities adoption among the urban poor. Information Technologies & International Development, 4(3), 57–73.  
  
3. Security and Maintenance Risks  
  
Although open source software allows for public inspection of the source code, it does not guarantee automatic updates or support. If not maintained properly, open source systems can be vulnerable to cyberattacks. Governments must actively monitor and patch these systems, or risk exposing sensitive data.

A [2018](tel:2018) report by the National Audit Office of Tanzania (NAOT) highlighted that several government systems—especially at the local level—lacked proper cybersecurity measures, regular updates, and formal support contracts. These vulnerabilities expose the systems to malware, data breaches, or service downtime, especially when external attacks occur.  
  
  
  
 Reference   
  
National Audit Office of Tanzania. ([2018](tel:2018)). Annual General Report of the Controller and Auditor General on the Audit of Local Government Authorities for the Financial Year [2016](tel:2016)/[2017](tel:2017). Retrieved from <https://www.nao.go.tz>/

4. Fragmentation and Lack of Standardization  
  
Different government ministries may adopt different open source systems without coordination, leading to fragmented systems that do not easily share data. This lack of interoperability can result in inefficiencies and duplication of efforts.

Example in Health sectors; District Health information System and Region Health information Sytem have implemented separated.

Reference:  
Nkohkwo, Q. N., & Islam, M. S. ([2013](tel:2013)). Challenges to the Successful Implementation of e-Government Initiatives in Sub-Saharan Africa: A Literature Review. Electronic Journal of e-Government, 11(1), [253](tel:253)–[267](tel:267).  
  
  
  
  
  
  
5. Limited Support and Accountability  
  
Unlike commercial software, which comes with vendor-backed customer support, open source tools often rely on community forums or independent contractors. This can be unreliable in mission-critical government systems where guaranteed uptime and quick issue resolution are needed.  
  
Reference:  
Ghosh, R. A. ([2005](tel:2005)). Understanding Free Software Developers: Findings from the FLOSS Study. In D. G. Messerschmitt (Ed.), Economic Perspectives on Free and Open Source Software (pp. 23–46). MIT Press.