CLOUD COMPUTING GUIDELINES

FOR FINANCIAL SERVICE PROVIDERS, 2023

BANK OF TANZANIA

FEBRUARY 2023

TABLE OF CONTENTS

PART I
Introduction and Background

1. These guidelines shall be cited as "*Cloud Computing Guidelines for Financial Service Providers, 2023.*"
2. These Guidelines are issued under Section 70(3) of the Bank of Tanzania Act, 2006.
3. These guidelines shall apply to all financial service providers intending to adopt cloud computing solutions for peripheral systems except where prescribed otherwise by the Bank in other Guidelines or Regulations.
4. Outsourcing of cloud computing solutions for mission-critical systems shall be in line with the requirements of the guideline 10(g) of *the Outsourcing Guidelines for Banks and Financial Institutions, 2021.*
5. In these Guidelines, unless the context otherwise requires:

   "Act" means the Bank of Tanzania Act;
   "Bank" means the Bank of Tanzania;
   "bank" has the same meaning ascribed to it in the Act;
   "financial institution" has the same meaning ascribed to it in the Act;
   "financial service provider" means an Institution licensed, regulated and supervised by the Bank
6. For the purpose of these guidelines, application systems of financial service providers shall be classified as (1) mission critical or (2) non-mission critical (peripheral system).

   a) Mission Critical Systems

   A mission critical system is a system that is essential to the survival of a business or organization. When a mission critical system fails or is interrupted, business operations are significantly impacted. Mission-critical computing, also known as a

mission-critical system, is any IT component (software, hardware, database, process, application, etc.) that performs a function essential to business operation. These systems enable financial service provider perform functions such as:

(i) Core management functions including customer deposit mobilization, granting of credit, trade finance, payments and settlements, corporate planning, control and decision-making functions;

(ii) Determining compliance with Anti-Money Laundering and Combating of Financing of Terrorism and Know Your Customer (KYC) norms for opening accounts; and

(iii) Treasury function.

In line with guideline 10(g) of *the Outsourcing Guidelines for Banks and Financial Institutions, 2021, financial* service providers shall not host in a primary data center outside Tanzania any mission-critical system or any other system, whose data are considered critical for the operations of an institution.

b) Non-mission critical (peripheral system)

A non-mission critical system that is also termed a peripheral system refers to a system, which is not essential to the core operations of a financial service provider. These systems support functions that are important to the Financial service provider's business but are not critical to its ability to function and serve its customers. These systems enable financial service providers to perform the functions such as marketing and sales, human resource management, budgeting, and collaboration.

PART II
Evaluation Criteria for Approval

7. Financial Service Provider that is planning to adopt cloud computing for peripheral system or is planning to vary any cloud computing arrangement shall seek prior written approval of the Bank.
8. These guidelines provide criteria for evaluation of applications from financial service provider intending to host peripheral system to the cloud. The minimum criteria that the Bank of Tanzania may take into consideration in evaluating requests from financial service providers intending to adopt cloud computing for peripheral systems shall include the following:
    a) Demonstration of the need for the adoption of cloud computing including the costs and benefits of such arrangement;
    b) Details of the dataset that the proposed cloud solution will retrieve, capture, persist, and disseminate, this includes source and destination systems. Further, the submission shall include the details of hosting of the source and destination systems;
    c) A clear basis for determining the fees payable and methodology for allocating costs of shared services;
    d) Potential impact of cloud computing arrangements on the financial service provider’s tariff structure;
    e) Evidence of due diligence on the capacity of the cloud computing service provider, which shall include:

(i) Strong security measures in place to protect data in transit and at rest, including encryption, multi-factor authentication, and strict access controls.

(ii) Ability to demonstrate compliance with relevant laws and regulations, including data privacy regulations and industry-specific regulations such as those governing the handling of sensitive financial information.

(iii) Track record of uptime and availability, as downtime, can have significant financial consequences to the financial service provider.

(iv) Capacity to handle the workload required by the financial service provider.

(v) Ability to scale up or down to meet the changing needs of the financial service provider, providing flexibility and cost-effectiveness.

(vi) Ability to offer competitive pricing and a clear, transparent billing structure.

(vii) Ability to offer a high level of technical support and customer service, with dedicated support staff available to assist with any issues that may arise.

(viii) Ability to seamlessly integrate with the financial service provider's existing systems and processes, where necessary.

(ix) Ability to customize and tailor its services to meet the specific needs of the financial service provider.

(x) The technology in use has no vendor locking and financial service provider can migrate the outsourced cloud service to on-premises or other cloud computing provider;

f) Potential impact of the adoption of cloud computing on earnings, solvency, liquidity, funding, capital and risk profile;

g) Aggregate exposure to a particular cloud computing service provider in cases where financial service provider hosts various peripheral systems to the same cloud computing service provider; and

h) Ability to maintain appropriate internal controls and meet regulatory requirements, even if there are operational problems faced by the cloud computing service provider.

PART III
Cloud Computing Contract

9. All cloud computing arrangements shall be subject to a written contract, which must be approved by the Bank before implementation.
10. The contract shall be reviewed by the financial service provider's legal counsel to ensure that it is legally enforceable and that it protects financial service provider from risk.
11. The financial service providers shall ensure that the written cloud computing contract(s) contain, among others, provisions pertaining to:
    a) The scope of services and level of performance that the cloud service provider will provide.
    b) Provisions to enforce oversight and monitoring of cloud computing service provider.
    c) The Bank's right to access at any time records of transactions and any information given to, stored at or processed by the cloud computing service provider, any report or any results of audits and security reviews on the cloud computing service provider and any sub-contractor that the cloud computing service provider may use;
    d) Right to audit or receive audit reports conducted by independent third parties.
    e) Availability of information to allow for regulatory oversight.
    f) Exit strategies and clear termination procedures.
    g) Controls with regard to data availability, privacy and confidentiality, and integrity.

h) Contingencies including infrastructure redundancy and backup arrangements to ensure business continuity;

i) Notification requirements for any material changes to issues pertaining to underlying platforms, hardware, systems, controls, and contact person that facilitate delivery of cloud computing services;

j) Roles and responsibilities in administering and protecting the cloud computing solutions; and

k) Dealing with the expected or unexpected termination of a contract and other cloud computing service interruptions.

PART IV
Cloud Computing Policy

12. The financial service provider shall have a general policy on its approach to all aspects of cloud computing solution. To be effective, the policy must be communicated in a timely manner and shall be implemented through all relevant levels of the financial service provider, and be revised periodically in line with changes in circumstances and applicable laws.

13. The cloud computing policy, at minimum, shall:

    a) cover the mechanism for appropriate monitoring and assessment of the cloud computing solution by the financial service provider;

    b) specify an internal unit or individual responsible for supervising and managing each cloud computing solution;

    c) specify arrangement and modalities of recovering the resources such as data, in case of any dispute on the contract or political imbalances;

    d) cover well-defined acquisition process with evaluation components such as terms of reference document, specification of requirements and evaluation of proposals;

    e) provide for initial and periodic due diligence on the cloud computing service provider;

    f) cover the financial service provider's plan and implementation arrangements to maintain the continuity of its business in the event that the provision of services by a cloud computing service provider fails or deteriorates to an unacceptable degree, or experiences other changes or problems;

g) include some form of contingency planning and the establishment of a clearly defined exit strategy, evaluated against the costs and benefits of such planning; and

h) require the financial service provider to manage the risks associated with its cloud computing arrangements.

14. financial service provider shall submit the cloud computing policy to the Bank for clearance before its implementation.

Dodoma,

____/____ /2023

Emmanuel Mpawe Tutuba

Governor