CLOUD COMPUTING GUIDELINES FOR FINANCIAL SERVICE PROVIDERS, 2023

BANK OF TANZANIA

December 2023

TABLE OF CONTENTS

PART I 1

Introduction and Background 1

PART II 3

Evaluation Criteria for Approval 3

PART III 6

Cloud Computing Contract 6

PART IV 8

Cloud Computing Policy 8

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 71 of *the Banking and Financial Institutions Act, 2006* and section 56(3) of the *National Payment Systems Act, 2015*.

3. These Guidelines shall be applied in evaluating applications from financial service providers intending to adopt cloud computing solutions.

4. In these Guidelines, unless the context otherwise requires:

   "Bank" means the Bank of Tanzania;

   "Financial service provider" means an institution licensed, regulated, and supervised by the Bank.

5. Cloud computing allows an Institution to outsource Information Technology (IT) systems that can be accessed via the internet, rather than hosting its own IT systems by lump sum investment in databases, software, and hardware. Further, cloud computing is the practice of using a network of remote servers hosted on the internet by a third party to store, manage, and process data, rather than a local server in the institution or a personal computer.

6. Cloud services are normally offered by third parties and can be made available for public use (Public Cloud), limited use (Private Cloud) or a combination of the two (Hybrid). Regardless of the type of cloud hosting option adopted, the requests from a Financial Service Provider intending to adopt a cloud computing solution shall be evaluated against data residence and exposure to cybersecurity threats and risks amongst other parameters. Other evaluation parameters are as provided under guideline 9 of these Guidelines.

7. For the purpose of these Guidelines, application systems of a financial service provider shall be classified as (1) mission critical system or (2) non-mission critical system.

(a) Mission Critical System

A mission critical system is a system that is essential to the survival of a financial service provider. When a mission critical system fails or is interrupted, business operations are significantly impacted. Mission-critical is any IT component (software, hardware, database, process, application, etc.) that performs a function essential to business operation. These systems enable a financial service provider to perform Core management functions including customer deposit management, granting of credit accommodations, trade finance, payments and settlements, and human resource management.

A financial service provider shall not host a mission-critical system or any other system whose data are considered critical for the operations of the financial service provider as determined by the Bank, in a primary data centre or cloud service provider whose hosting infrastructure is outside the United Republic of Tanzania.

(b) Non-mission critical

A non-mission critical system is a system that is not essential to the core operations of a financial service provider. These systems enable a financial service provider to perform the functions such as marketing and sales, budgeting, and collaboration.

PART II

Evaluation Criteria for Approval

8. A financial service provider that is planning to adopt cloud computing for non-mission critical system or is planning to vary any cloud computing arrangement shall seek prior written approval of the Bank.

9. These Guidelines provide criteria for evaluation of applications from financial service providers intending to host non-mission critical system to the cloud. The minimum criteria for evaluating requests from the financial service provider intending to adopt cloud computing for non-mission critical systems shall include the following:

   (a) Demonstration of the need for the adoption of cloud computing including the costs and benefits of such arrangement. The anticipated costs shall indicate names of all cloud services acquired, and should be spread over a period of five years plan with a cost comparison over the same period for on premise arrangement.

   (b) Details of 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 providers 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, identification and remediation of vulnerabilities, 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; and

(x) The technology in use has no vendor locking and the 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 the financial service provider hosts various non-mission critical 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

10. All cloud computing arrangements shall be subject to a written contract, which must be approved by the Bank before implementation.

11. The contract shall be reviewed by the financial service provider's legal counsel to ensure that it is legally enforceable and that it reasonably protects the financial service provider from risk.

12. The financial service provider shall ensure that the written cloud computing contract(s) contain, among others, provisions pertaining to:

    (a) The scope of services that the cloud service provider will provide;

    (b) Service Level Agreement (SLA) with the cloud service provider;

    (c) Provisions to enforce oversight and monitoring of the cloud computing service provider;

    (d) 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;

    (e) Right to audit or receive audit reports conducted by independent third parties;

    (f) Availability of information to allow for regulatory oversight;

    (g) Exit strategies and clear termination procedures including clear provision in dealing with events of winding up, insolvency or regulatory takeover of cloud computing service provider;

    (h) Controls with regards to data availability, privacy and confidentiality, and integrity;

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

(j) 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;

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

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

PART IV

Cloud Computing Policy

13. 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 reviewed annually.

14. In setting up the policy, the financial service provider shall bear in mind that no cloud computing service is risk-free. Therefore, at minimum, the cloud computing policy 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 unrest;

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

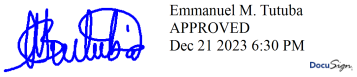
    (e) provide for initial and periodic due diligence at least annually or more frequently in line with changes in circumstances on the cloud computing service provider;

    (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.

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



Emmanuel Mpawe Tutuba

GOVERNOR