MATRIX OF CHANGES

DRAFT REVISED CLOUD COMPUTING GUIDELINES FOR FINANCIAL SERVICE PROVIDERS

BANK OF TANZANIA

August 2025

		Stakeholders Comments	Team Proposal	Revised Guideline
	PART I			
	Introduction and Background			
	1. These guidelines shall be cited as "*Cloud Computing Guidelines for Financial Service Providers, 2023*"	None		These guidelines shall be cited as "*Cloud Computing Guidelines for Financial Service Providers, 2025*"
	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.	None		
	3. These guidelines shall be applied in evaluating applications from financial service providers intending to adopt cloud computing solutions.	None		
	4. In these Guidelines, unless the context otherwise requires:	None		
	"Bank" means the Bank of Tanzania;	None		
	"Financial service provider" means an institution	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	licensed, regulated, and supervised by the Bank.			
	5. Cloud computing allows an Institution to outsource 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.	None		
	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			

		Stakeholders Comments	Team Proposal	Revised Guideline
	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.	None		
	a) Mission Critical Systems	None		
	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	The definition of mission critical systems is very wide and covering majority of the banking systems. Some of these systems will perform better on the cloud compared to on premise computing. Therefore, we suggest some of the mission critical systems to be reclassified and allowed on cloud computing on risk-based approach and approval from the Bank.	The definition of a mission-critical system is comprehensive and well-articulated. It aligns with similar definitions adopted by other SADC member states as well as India and Mauritius (*material outsourcing*), and therefore, it is recommended that the same definition to prevail after deleting the examples;	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,

		Stakeholders Comments	Team Proposal	Revised Guideline
	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.	The expected functions of mission-critical system should be exhaustive to make it clear.		process, application, etc.) that performs a function essential to business operation. These systems enable a financial service provider to perform core functions.
	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 FSP as determined by the Bank, in a primary data Centre or Cloud service provider whose hosting infrastructure is outside Tanzania.	None		
	b) Non-mission critical	None		
	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.	Since the list of functions of the non-mission critical is not finite, we suggest that there should be a clear avenue of verifying whether something is mission critical or not (say: no Personal, Client or transactional data, etc).	1. The definition of non-mission critical system highly depends on the definition of mission-critical system and therefore since it is recommended to maintain the same definition of mission-critical systems, then the	A non-mission critical system refers to a system that is not essential to the core operations or survival of a financial service provider. Its failure or interruption does not significantly impact business continuity.

		Stakeholders Comments	Team Proposal	Revised Guideline
			same definition for non-mission critical systems may also prevail; 2. The Bank of Tanzania cannot exhaustively provide a list of non-mission-critical systems; 3. Regulation 42 of the Payment Systems (Licensing and Approval) Regulations, 2015 provides that a payment system provider shall place its primary data center in relation to payment system services in Tanzania. Further, Guideline 10(g) of the Outsourcing Guidelines for Banks and Financial Institutions, 2021 provides that banks and financial institutions shall not outsource Primary data centre outside the country.	These systems typically support auxiliary functions.

		Stakeholders Comments	Team Proposal	Revised Guideline
	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.	Provided that the system is identified to be non-mission critical via clear process / criteria; we suggest that Financial Institutions to only send notification for adopting cloud computing for the non-mission critical system. Approval process is likely to have delays that will hold up the Financial Service Provider to get the benefits of cloud computing system in time. Also, such identified non-mission critical systems can be made available to the banks so that they are known for their proper action. It was also noted that some of the Financial Service Providers already had several systems and applications that were hosted on cloud prior to the issue of	1. Financial Service Providers (FSPs) seeking prior approval is essential, as such review requests enable the Bank of Tanzania to reassess the risks associated with the adoption of cloud computing before the FSP enters into a contract with a Cloud Service Provider. This process helps prevent potential costs arising from contract termination due to unforeseen regulatory or risk concerns. Furthermore, the Bank should ensure timely responses to FSPs' approval requests, in accordance with its established turnaround time, to enable FSPs to realize the benefits of cloud computing systems without unnecessary delays;	10.A financial service provider who, before the commencement of these Guidelines, had a system or an application that is hosted on cloud shall within twelve months of commencement of these Guidelines apply for a written approval from the Bank or cease the adoption of cloud computing in accordance with these Guidelines.

		Stakeholders Comments	Team Proposal	Revised Guideline
		the guidelines. These systems are currently in use. We are ready to provide a list of the systems/ applications and what they do for further discussions.	2. The Cloud Computing Guidelines were designed for non-mission critical systems, and hosting mission-critical systems in the cloud is prohibited. Therefore, allowing banks to continue hosting non-mission critical systems in the cloud without seeking approval could be interpreted as an intention to revoke the Guidelines; 3. Added guideline 10 to cater for transition arrangement for financial service providers who adopted cloud computing prior to issuance of the Guidelines.	
	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	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	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.	None		
	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			

		Stakeholders Comments	Team Proposal	Revised Guideline
	and destination systems.			
	c) A clear basis for determining the fees payable and methodology for allocating costs of shared services.	Since fees are commercially negotiated between Cloud Service Provider and Financial Service Provider; there is usually a Non-Disclosure Agreement (NDA) clause not to allow this to be shared.	Section 33(1) of *the Banking and Financial Institutions Act, 2006* provides that Notwithstanding any provision to the contrary contained in any written law, the Bank shall have power to access to any oral and documented information, including information in computers, books, minutes, accounts, cash, securities, documents, vouchers as well as any other things in the possession or custody or under the control of a bank or financial institution or its affiliate, which relate to the business of such bank or financial institution. Further, this is also the requirements of Guideline 7(b) of the Outsourcing Guidelines for Banks and Financial Institutions, 2021. Therefore, the provision	

		Stakeholders Comments	Team Proposal	Revised Guideline
			is enforceable and should prevail..	
	d) Potential impact of cloud computing arrangements on the financial service providers tariff structure.	None		
	e) Evidence of due diligence on the capacity of the cloud computing service provider, which shall include:	None		
	(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.	None		
	(ii) Ability to demonstrate compliance	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	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.	None		
	(iv) Capacity to handle the workload required by the financial service provider.	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	(v) Ability to scale up or down to meet the changing needs of the financial service provider, providing flexibility and cost-effectiveness.	None		
	(vi) Ability to offer competitive pricing and a clear, transparent billing structure.	None		
	(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.	None		
	(viii) Ability to seamlessly integrate with	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	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.	None		
	(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;	Some of the technologies are provided by the same Cloud Service Provider (CSP) and hence cannot be migrated to other CSP and migrating them to On-premises will defeat the Cloud technology advantages: Scalability, Resiliency, Cost, etc. Example: Microsoft Office 365 can only be hosted in Microsoft Azure Cloud. We suggest risk assessment to be done and mitigation	The provision grants financial service providers a flexibility to disengage from existing cloud computing vendors, while ensuring business continuity in the event of a separation with the cloud service provider.	

		Stakeholders Comments	Team Proposal	Revised Guideline
		provided on a specific vendor.		
	f) Potential impact of the adoption of cloud computing on earnings, solvency, liquidity, funding, capital and risk profile;	None		
	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	As of now, there are only a few reputable Cloud Service Providers (eg: Microsoft & Amazon) which means narrow range of choices for Financial Service Providers. Also, these CSP's have already proved to be reliable technologically, financially etc. We suggest this part to be re-looked based on the limitations.	The Guideline intends to manage the concentration risk to avoid Single point of failure.	
	h) Ability to maintain appropriate internal controls and meet regulatory requirements, even if there are operational problems faced by the cloud computing service provider.	None		
			Added item (j) on the need for financial service	j) The impact on the Financial Service

		Stakeholders Comments	Team Proposal	Revised Guideline
			provider to conduct an assessment on the impact on financial service provider reputation in case the service provider fails.	Provider's reputation in the event of service provider failure, and the adequacy of the identified fallback position or backup arrangements to address such failure;
			Added guideline 10 to cater for transition arrangement for financial service providers who adopted cloud computing prior to issuance of the Guidelines.	10. A financial service provider that, before the commencement of these Guidelines, had adopted cloud computing shall within twelve months of commencement of these Guidelines apply for a written approval from the Bank or cease the adoption of cloud computing in accordance with these Guidelines.
	PART III			
	Cloud Computing Contract			
	11. All cloud computing arrangements shall be	For International Financial Service Providers, it is	For the service entered at a group level,	

		Stakeholders Comments	Team Proposal	Revised Guideline
	subject to a written contract, which must be approved by the Bank before implementation.	efficient for such contracts to be done at Group level as opposed to country in order to realise, among other benefits, the economies of scale. To some of the Financial Service Providers the cloud contracts are negotiated, done and maintained at group level.	Financial Service Providers are required to have a separate agreement which complies with the Guidelines requirements. Further, this is in line with *the Outsourcing Guidelines for Banks and Financial Institutions, 2021*.	
	12. 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.	None		
	13. The financial service provider shall ensure that the written cloud computing contract(s) contain, among others, provisions pertaining to:	None		
	a) The scope of services that the cloud service provider will provide.	None		
	b) Service Level Agreement (SLA)	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	with the cloud service provider.			
	c) Provisions to enforce oversight and monitoring of the cloud computing service provider.	None		
	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;	None		
	e) Right to audit or receive audit reports conducted by independent third parties;	None		
	f) Availability of information to allow for regulatory oversight;	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	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;	None		
	h) Controls with regards to data availability, privacy and confidentiality, and integrity;	None		
	i) Contingencies including infrastructure redundancy and backup arrangements to ensure business continuity;	None		
	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;	In Cloud computing we are subscribing to the service (say: MS Office 365) and hence interested in the performance of the service that is delivered to the Bank rather than the micro details regarding the peripheral systems that are used to support the service. In view of this, we propose	The provision intends to ensure that the cloud service provider continue to provide service smoothly even in case of changes pertaining to underlying platforms, hardware, systems, controls, and contact person.	Notification requirements for any material changes to that may impact availability of service provided by cloud service provider.

		Stakeholders Comments	Team Proposal	Revised Guideline
		that changes in underlying platforms, hardware, systems, controls, and contact person that facilitate delivery of cloud computing service should not require notification as long as the change does not result in material impact to the Financial Institutions.		
	k) Roles and responsibilities in administering and protecting the cloud computing solutions; and	None		
	l) Dealing with the expected or unexpected termination of a contract and other cloud computing service interruptions;	None		
			Added guideline 14 to cater for requirements for annual review of the financial and operational condition of the Cloud Service Provider.	14. A financial service provider shall, at a minimum, conduct an annual review of the financial and operational condition of the Cloud Service Provider to

		Stakeholders Comments	Team Proposal	Revised Guideline
				assess its continued ability to deliver cloud computing services. Such due diligence shall be based on all reasonably available information and shall identify any material deterioration in performance, breaches of confidentiality or security obligations, or deficiencies in business continuity preparedness
	PART IV			
	Cloud Computing Policy			
	15. 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	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	all relevant levels of the financial service provider, and be reviewed annually.			
	16. 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:	None		
	a) cover the mechanism for appropriate monitoring and assessment of the cloud computing solution by the financial service provider;	None		
	b) specify an internal unit or individual responsible for supervising and managing each cloud computing solution;	None		
	c) specify arrangement and modalities of recovering the	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	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;	None		
	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;	None		
	f) cover the financial service provider's plan and implementation arrangements to	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	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	None		
	h) require the financial service provider to manage the risks associated with its cloud	None		

		Stakeholders Comments	Team Proposal	Revised Guideline
	computing arrangements.			
	17. A financial service provider shall submit the cloud computing policy to the Bank for clearance before its implementation.	None		
			Added PART V General Provision to cover sanctions and revocation of previous Guidelines issued in 2023.	
			Added Guideline 17 on Sanctions for Non Compliance with the Guidelines.	18. Without prejudice to the other penalties and actions prescribed by the Act, the Bank may impose one or more of the following sanctions where any of the provisions herein are contravened: - (a)civil money penalty on the financial service provider or directors, officers

		Stakeholders Comments	Team Proposal	Revised Guideline
				or employees responsible for non-compliance in such amounts as may be determined by the Bank; (b) prohibition from engaging in cloud computing arrangements; (c) suspension of access to the credit facilities of the Bank; (d) suspension of lending and investment operations; (e) suspension of capital expenditure; (f) suspension of the privilege to accept new deposits; (g) suspension from office of the defaulting director, officer or employee; (h) disqualification from holding any

		Stakeholders Comments	Team Proposal	Revised Guideline
				position or office in any financial service provider regulated and supervised by the Bank of Tanzania; and (i) revocation of license issued by the Bank.
			Added guideline 18 revoking the Guidelines issued in 2023.	19. Cloud Computing Guidelines for Financial Service Providers, 2023 are hereby dis-applied