



DRAFT GUIDANCE NOTE ON THIRD-PARTY TECHNOLOGY SERVICE PROVIDERS

AUGUST 2026

TABLE OF CONTENTS

PART I: PRELIMINARY	4
1.1 Title	4
1.2 Application.....	4
1.3 Authorization.....	4
1.4 Definitions	4
PART II: STATEMENT OF POLICY	6
2.1 Purpose.....	6
2.2 Scope.....	6
2.3 Responsibility.....	7
2.4 Overview of Third-Party Technology Service Providers in the Banking Sector	7
PART III: LEGAL REQUIREMENTS RELATING TO RELIANCE ON THIRD PARTIES.....	12
3.1 Banking Act (Cap.488).....	12
3.2 Microfinance Act (Cap 493C).....	12
3.3 Risk Management Guidelines	12
3.4 Guidance Note on Cybersecurity for the Banking Sector.....	12
3.5 Proceeds of Crime and Anti-Money Laundering (POCAML) Regulations, 2023	13
3.6 Data Protection Act, 2019	15
3.7 Consumer Protection Act, 2012 (Cap.501)	15
PART IV: SPECIFIC REQUIREMENTS	16
4.1 Governance Framework	16
4.2 Role of Risk Management Functions.....	17
4.3 Independent Review and Audit	17
4.4 Legal obligations.....	18
4.5 Internal Controls and Standard of Care.....	18
4.4 Third-Party Technology Service Providers Risk Management Lifecycle.....	19
4.4.1 Identification and Assessment of Critical Services	19
4.4.2 Pre-Contractual Analysis and Due Diligence.....	20
4.4.3 Contract Stage	21
4.4.4 Onboarding.....	23
4.4.5 Monitoring	23
4.4.6 Risk Management.....	24

4.4.7	Exit and Transition	24
4.6	Cybersecurity in Third-Party TSP Arrangements	25
4.7	Data Protection in Third-Party TSP Arrangements	26
4.8	AML/CFT/CPF Compliance in Third-Party TSP Arrangements	26
4.9	Business Continuity	27
4.10	Intragroup Third-Party TSP Arrangements	27
4.11	Additional Requirements for Cloud Computing Arrangements.....	28
PART V: REPORTING		29
REFERENCES		32
ANNEX I: High-Level Contents of a Third-Party Technology Service Providers Policy		34
ANNEX II: Third-Party Technology Service Provider Checklist.....		35
ANNEX III: Third-Party TSPs Register (Annual).....		45
ANNEX IV: Third-Party TSP Incident Record (Immediate).....		46
ANNEX V: Third-Party TSP Incident Record (Final)		47
ANNEX VI: Third-Party TSP Incident Record (Quarterly)		49

PART I: PRELIMINARY

1.1 Title - Guidance Note on Third-Party Technology Service Providers

1.2 Application - This Guidance Note applies to all institutions licensed under the Banking Act (Cap. 488), the Microfinance Act (Cap. 493C), and Non- Operating Holding Companies (NOHCs), herein collectively referred to as “financial institutions” or “institutions”.

1.3 Authorization - This Guidance Note is issued under Section 33(4) of the Banking Act (Cap. 488) and Section 48(2A) of the Microfinance Act (Cap. 493C), which empowers the Central Bank of Kenya (CBK) to issue guidelines to be adhered to by institutions in order to maintain a stable and efficient banking system and deposit-taking microfinance system, respectively.

1.4 Definitions - The terms and acronyms used in this Guidance Note are defined below:

1.4.1 “Cloud” or “Cloud Computing” means a computing system that supports business and delivery models that enable on-demand access to a shared pool of resources such as applications, servers, storage and network security. Cloud computing is typically delivered in three forms, namely, Software as a Service (“SaaS”), Platform as a Service (“PaaS”) and Infrastructure as a Service (“IaaS”).

1.4.2 “Cloud Service Provider (CSP)” means a third-party technology service provider who provides cloud computing services to an institution.

1.4.3 “Critical Service” means a service provided to a financial institution whose failure or disruption could significantly impair a financial institution’s viability, critical operations, or its ability to meet key legal and regulatory obligations.

1.4.4 “Critical Third-Party Technology Service Provider” means third-party technology service provider who provides a critical service to an institution.

1.4.5 “Fourth-Party Service Provider” means a service provider that provides services to one or more third-party service providers, and this concept can be further extended into nth-party service providers.

1.4.6 “Intra-group service provider” means a service provider that is part of a financial institution’s group and provides services predominantly to entities

within the same group. Intra-group service providers may include a financial institution's parent undertaking, sister companies, subsidiaries, service companies or other entities that are under common ownership or control.

1.4.7 "Intragroup outsourcing" means an outsourcing arrangement under which an institution outsources a technology function or service to a parent, subsidiary, affiliate or any other entity within the same corporate group or financial conglomerate.

1.4.8 "Intragroup technology service provider" means a parent undertaking, subsidiary, affiliate or other entity within the same corporate group or financial conglomerate that provides ICT services to an institution under an intragroup service arrangement.

1.4.9 "Nth-party service provider" means a service provider that is part of a third-party service provider's supply chain and supports the ultimate delivery of services to one or more financial institutions.

1.4.10 "Material incident" means any incident associated with a third-party technology service provider arrangement that materially affects, or is reasonably likely to materially affect, the institution's operations, critical services, information assets, customers, or compliance with this Guidance and applicable laws and regulations.

1.4.11 "Outsourcing" means a category of third-party service relationship(s) where a financial institution uses a service provider to perform, on a recurrent or an ongoing basis, services, or parts thereof, that would otherwise be undertaken, or could reasonably be undertaken, by the financial institution itself.

1.4.12 "Service Level Agreement (SLA)" means a contract between a service provider and a customer that defines the service to be provided and the level of performance to be expected. An SLA also describes how performance will be measured and approved, and what happens if performance levels are not met.

1.4.13 "Supply chain" means the network of entities that provide infrastructure, physical goods, services and other inputs directly or indirectly utilised for the delivery of a service to a financial institution.

1.4.14 "Third-party service provider" means a service provider that provides services to one or more financial institutions under a third-party service relationship.

1.4.15 “Third-Party service relationship” means a formal arrangement for the provision of one or more services, or parts thereof, to a financial institution by a service provider.

1.4.16 “Third-Party Technology Service Provider (TSP)” means an external entity, either a person or company, that provides technology services to an organization under a contractual agreement, such as cloud storage, software applications, or Information Technology (IT) infrastructure.

PART II: STATEMENT OF POLICY

2.1 Purpose

This Guidance Note outlines the minimum requirements for the engagement, management, and oversight of Third-Party Technology Service Providers (TSPs) by financial institutions. The Guidance Note aims to: -

- a) Address emerging risks such as cyber threats, operational disruptions, and cross-border dependencies.
- b) Strengthen financial institutions’ resilience by requiring appropriate risk management, due diligence, and oversight of TSPs.
- c) Promote consistency across financial institutions in managing third-party relationships.
- d) Strengthen consumer protection by safeguarding customer data, privacy, and interests in line with applicable laws and global best practices.
- e) Provide supervisory clarity on outsourcing arrangements and reporting obligations by financial institutions.
- f) Foster public trust and confidence in the banking system, which is essential for financial inclusion and economic growth.

2.2 Scope

This Guidance Note sets out the minimum standards that commercial banks and microfinance banks (MFBs) should adopt when engaging Third-Party Technology Service Providers. It is not a replacement for and does not supersede the legislation, regulations and guidelines that institutions must comply with as part of their regulatory obligations, particularly in the areas of risk management, outsourcing, information communication technology, internal controls and corporate governance.

2.3 Responsibility

The Board of Directors and senior management of financial institutions bear the primary responsibility for ensuring management of outsourcing relationships with third-party TSPs. This includes establishing appropriate governance structures, due diligence processes, and risk management frameworks to safeguard institutional resilience. These aspects of third-party TSPs must be documented and made available for review by external auditors and CBK.

2.4 Overview of Third-Party Technology Service Providers in the Banking Sector

The Kenyan financial sector has witnessed an acceleration in the adoption of digital financial services, driven by digital transformation, increased customer demand for efficient services, and the need for cost optimization. This evolution has been largely enabled by third-party TSPs who provide vital technological services to financial institutions. TSPs enable institutions to increase revenues, reduce costs, improve operational resilience, and quickly scale products and services.

The landscape of TSPs serving the Kenyan banking sector encompasses a wide range of services, including:

- a) Cloud computing services.
- b) Custom software applications.
- c) Information Technology (IT) infrastructure.
- d) Payment technology services.
- e) Cybersecurity services.
- f) Data analytics.
- g) Digital platforms.
- h) Managed IT services.
- i) Data centre and colocation services.
- j) Data and analytics services.
- k) Network and telecommunications services.
- l) Identity and trust services.

The reliance on TSPs has enhanced efficiency, broadened financial inclusion, and supported product innovation. However, dependency on TSPs introduces significant risks, including operational, cyber-security, compliance, and reputational risks.

2.4.1 Cloud Computing

Cloud computing is a subset of third-party technology service providers. Cloud computing can be described by their characteristics, service models, and deployment models.

a) Characteristics of Cloud Computing

The typical characteristics of cloud computing are outlined below.

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction with each service provider.
- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by multiple client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling.** The provider's computing resources are consolidated to serve multiple consumers using a multi-tenant model (single instance of software runs on a server and serves multiple tenants), with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the consumers generally have no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity.** Capabilities can be provisioned and released flexibly, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service.** Cloud systems automatically control and optimize use of resources by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

b) Cloud Computing Service Models

Cloud computing can be categorised by their service models as outlined below.

- **Software as a Service (SaaS).** The capability provided to the consumer is to use the cloud provider's applications running on a cloud infrastructure¹. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Platform as a Service (PaaS).** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the cloud provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **Infrastructure as a Service (IaaS).** This model provides the consumer with processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

c) Cloud Computing Deployment Models

Cloud computing can be categorised by their deployment models as outlined below.

- **Private cloud:** The cloud infrastructure is provided for exclusive use by a single organization. It may be owned, managed, and operated by the organization, a third-party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provided for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third-party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provided for open use by the general public. It may be owned, managed, and operated by a business, academic, government

¹ A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

organization, or some combination of them. It exists on the premises of the cloud provider.

- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud deployment models (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.
- **Multicloud:** The use of two or more different public cloud providers to handle different workloads, offering redundancy and preventing vendor lock-in.

2.4.2 Third-Party Technology Service Providers in the Kenyan Banking Sector

CBK recognizes TSPs as enablers of modern banking services. However, there is need for governance, oversight, and contingency planning to mitigate potential disruptions and safeguard the stability of the financial system.

CBK conducted a survey on third-party TSPs to commercial banks and MFBs in March 2025. The survey aimed to provide a comprehensive analysis on the use of TSPs in the Kenyan banking sector, focusing on the current state, benefits, risks and future trends. The survey was geared towards providing valuable insights into how the banking sector can leverage third-party technology service providers to drive innovation while identifying any existing gaps and understanding future trends. The key survey findings are indicated below.

- a) All commercial banks and MFBs indicated that they relied on third-party TSPs in their operations.
- b) Commercial Banks use TSPs to support key functions. The most cited services include cloud-based services, mobile-banking and internet banking. Meanwhile, MFBs noted that they engage third parties to support both core banking and mobile banking.
- c) 38 out of 52 respondents considered cybersecurity and data privacy concerns as the biggest challenges in engaging TSPs.
- d) 83 percent of surveyed institutions reported having a formal incident response plan in place for breaches or failures involving third-party technology service providers. Meanwhile 15 percent indicated that such plans were under development while 2 percent reported having no such plans in place.
- e) 100 percent of commercial banks and 93 percent of MFBs indicated that they had governance structures and frameworks for dealing with third parties. These typically included Third-Party Risk Management Committees, disclosure agreements, Service Level Agreements (SLAs), and incorporating third-party vendor training into their governance frameworks with third-party TSPs. Majority of the institutions also

required evidence of compliance with standards like ISO 27001,² PCI-DSS,³ or ISO 22301⁴ onboarding in their governance frameworks with TSPs.

- f) 89.5 percent of commercial banks had a clear process for incorporating lessons learned from incidents or audits into their third-party risk management frameworks. This indicated a strong focus on continuous improvement and structured risk management.
- g) 89 percent of commercial banks and 57 percent of MFBs responded that they had formal processes for identifying risks. Meanwhile approximately 12 percent of commercial banks and 43 percent of MFBs indicated that their processes for identifying third-party risk was in development.
- h) 79 percent of institutions surveyed reported using key performance indicators (KPIs) to monitor the performance of third-party TSPs. Out of those, 61 percent of institutions surveyed reported the KPIs to the board.
- i) 95 percent of commercial banks and 86 percent of MFBs conducted regular internal audits on third-party TSPs to identify gaps and ensure alignment with regulatory expectations.
- j) 32 percent of commercial banks and 14 percent of MFBs indicated that the current regulatory framework on outsourcing was supportive, while 7 percent of MFBs and 3 percent of commercial banks stated that the current regulations acted as a barrier towards adoption of third parties. Additionally, 66 percent of commercial banks and 79 percent of MFBs noted that the existing regulations, while supportive, could be improved.

Respondents to the survey recommended that CBK develops a clear regulatory framework on TSPs.

Recognizing these developments, CBK has issued this Guidance Note to financial institutions to strengthen supervisory oversight over outsourcing arrangements involving TSPs. This Guidance Note sets a proportional risk-based approach to the management of TSPs. The Guidance Note will ensure that the benefits of third-party collaborations are realized without undermining the institution's stability or the trust of its customers.

This Guidance Note has been developed in line with best practices by standard-setting bodies as well as practices in leading and comparative jurisdictions.

² ISO 27001 - an information security management standard that provides a structured framework for organizations to protect their information assets through the adoption of an information security management system.

³ PCI-DSS – a set of security standards designed to protect card transactions.

⁴ ISO 22301 – a security standard for business continuity management.

PART III: LEGAL REQUIREMENTS RELATING TO RELIANCE ON THIRD PARTIES

3.1 Banking Act (Cap.488)

Section 33(4) of the Banking Act empowers CBK to issue directions, including standards and guidelines, to institutions for implementation of the purposes and provisions of the Act. The Banking Act also imposes obligations relating to prudent management, maintenance of proper records, internal controls, and regulatory access to information, all of which continue to apply even where services are outsourced.

3.2 Microfinance Act (Cap 493C)

Section 4A of the Microfinance Act empowers CBK to issue guidelines, circulars, and directives to institutions for purposes of implementing the Act. The Act also imposes obligations concerning prudent operations, risk management, and maintenance of adequate systems and controls, which extend to outsourced functions and technology service providers.

3.3 Risk Management Guidelines

The Risk Management Guidelines complement the outsourcing framework by requiring institutions to establish comprehensive risk management systems covering operational risk, technology risk, cybersecurity risk, legal risk, reputational risk, and concentration risk arising from outsourcing arrangements. Institutions are expected to identify, assess, monitor, and mitigate risks associated with third-party service providers on an ongoing basis. The Guidelines emphasize that outsourcing may create operational vulnerabilities and dependencies that institutions must actively manage through robust governance and internal controls.

The risk management framework also requires institutions to maintain business continuity and disaster recovery capabilities. Institutions must ensure that outsourced technology arrangements do not expose them to unacceptable operational disruption in the event of service failure, cyberattack, insolvency of the provider, or termination of the outsourcing arrangement. Consequently, institutions are expected to maintain contingency arrangements, recovery plans, backup systems, and exit strategies for critical outsourced services.

3.4 Guidance Note on Cybersecurity for the Banking Sector

Section 3.3 of the CBK Guidance Note on Cybersecurity for the Banking Sector addresses outsourcing. It recognises that commercial banks increasingly rely on

outsourcing, cloud providers, and third-party service providers for operational efficiency. However, such arrangements introduce significant cyber and operational risks.

The Guidance Note requires institutions to ensure that third parties comply with applicable legal and regulatory frameworks and international best practices. Further, it requires commercial banks to maintain adequate governance over outsourcing arrangements. This is through proper due diligence, documented agreements, ongoing monitoring, vendor risk assessments, security and compliance controls, and robust service level agreements. Institutions are also required to understand and continuously assess the risks posed by each third-party, monitor changes in the vendor's cyber posture or business operations, collaborate with vendors to mitigate risks, and develop exit management and contingency plans for outsourced services.

3.5 Proceeds of Crime and Anti-Money Laundering (POCAML) Regulations, 2023

The POCAML Regulations, 2023, define third-party to mean another financial institution or designated non-financial business or profession or a person that is supervised or monitored by a competent authority. The competent authority referred herein is any public authority other than a self-regulatory body with designated responsibilities for combating money laundering and terrorism financing.

The meaning of the terms “financial institution” and “designated non-financial business or profession” are contained in section 2 of Proceeds of Crime and Anti-Money Laundering Act (Cap. 59A).

Regulation 33 of POCAML Regulations, 2023, permits a reporting institution to rely on a third-party to perform elements of Customer Due Diligence (CDD) measures or to introduce business, provided that the institution meets the criteria set out in the Regulations.

Regulation 33 of POCAML Regulations, 2023 does not expressly refer to technology service providers. However, third-party technology service providers may come within the scope of the reliance framework where a reporting institution relies on them to support or perform elements of CDD or to introduce business, and where the provider falls within the definition of a third-party under Regulation 33(9). Therefore, POCAML Regulations distinguish third-party reliance from ordinary outsourcing or agency arrangements.

Some of examples of technology enabled CDD services that require compliance with Regulation 33 considerations include; electronic identity verification, biometric verification, document authentication, beneficial ownership verification, sanctions

screening, politically exposed person screening, adverse media screening, automated risk scoring, customer onboarding support, collection or verification of identification data.

This should be differentiated to third-party technology providers for example who supplies software, hosting infrastructure, technical tools, cybersecurity risk service providers who may be treated primarily as an outsourcing.

Below are examples of scenarios of distinction between technology outsourcing and reliance on a third-party.

Arrangement	Features	Treatment
Technology vendor / software provider	Provides software, hosting, API connectivity, workflow tools, data storage or infrastructure. The reporting institution conducts and controls the CDD decision.	Primarily outsourcing, operational risk, cybersecurity, confidentiality and data protection obligations. Regulation 33 may not apply unless the provider performs CDD elements or introduces business.
Third-party KYC/CDD provider	Collects, verifies, screens, authenticates or assesses customer identification, beneficial ownership, sanctions, PEP status, risk rating or related CDD information.	Regulation 33 applies where the institution relies on the provider for CDD elements. The institution must ensure supervision/monitoring by a competent authority, written agreement, immediate information access and document availability without delay.
Intra-group third party	A related entity within the same financial group performs CDD elements or introduces business.	Regulation 33(8) applies. The group must apply CDD, record-keeping and AML/CFT/CPF programmes, be supervised at group level by a competent authority, and mitigate higher country risk through group policies.

3.6 Data Protection Act, 2019

The legal requirements on the protection of personal data are set out under the Data Protection Act, 2019. The Act establishes the principles of lawful processing, rights of data subjects, offences, and compliance obligations that apply to both data controllers and data processors, including third parties.

Section 30(1)(vii) of the Act provides that:

A data controller or data processor shall not process personal data unless for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject.

Section 40(2) of the Act provides for the right of rectification and erasure, with an obligation to inform third parties of data subject requests for rectification and erasure, as indicated below.

Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested:

- (a) the rectification of such personal data in their possession or under their control that is inaccurate, outdated, incomplete or misleading; or*
- (b) the erasure or destruction of such personal data that the data controller is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.*

3.7 Consumer Protection Act, 2012 (Cap.501)

The Consumer Protection Act, 2012 (Cap.501), places obligations on suppliers of goods and services to ensure fairness, transparency, and accountability in their dealings with consumers. Institutions that outsource services to third-parties remain responsible for ensuring that consumers' rights, such as access to information, fair contractual terms, and corrective actions, are enforced.

PART IV: SPECIFIC REQUIREMENTS

4.1 Governance Framework

4.1.1 Role of the Board of Directors

The board of directors holds the ultimate responsibility for approving policies on third-party arrangements and holding senior management accountable for implementation of the risk-management framework. In this regard, the board will undertake the following responsibilities:

- a) Establish the institution's policy on third-party TSPs, which at a minimum should contain the provisions set out in **Annex I**. The policy should be reviewed periodically in accordance with the institution's governance framework.
- b) Decide on the specific business activities to be outsourced and approve such arrangements.
- c) Ensure that the institution establishes a risk-evaluation framework for existing and potential outsourcing arrangements involving TSPs.
- d) Establish the chain of command and formal line of authority for seeking approval in outsourcing arrangements.
- e) Undertake regular review of TSPs outsourcing strategies and arrangements for their continued relevance, safety and soundness.
- f) Ensure outsourcing arrangements do not compromise institutional soundness, financial stability, or CBK's supervisory authority.
- g) Ensure third-party TSPs are subjected to the institution's cybersecurity framework.
- h) Allocate adequate resources, expertise, and systems to manage third-party TSPs and the risks of such outsourcing.
- i) Ensure independent review and audit for compliance with set policies. Review on a regular basis and at least once annually the implementation of the institution's third-party TSPs outsourcing framework, and the implementation plan, including adequacy of mitigating controls.

4.1.2 Role of Senior Management

Senior management should implement the third-party strategy and policy. The key responsibilities of senior management include:

- a) Establishing clear roles and responsibilities for managing third-party TSP arrangements throughout the third-party life cycle. This should involve allocating specific tasks to business units and creating clear channels for decision-making.
- b) Implementing the third-party TSPs policy and implementation plan.
- c) Oversee daily management of TSP relationships.

- d) Coordinating capacity-building initiatives and facilitating training for staff members on risks of third-party TSPs and the institution's TSPs policy.
- e) Informing bank personnel and other relevant stakeholders on the institution's third-party TSPs risk frameworks.
- f) Providing regular reports to the board on the institution's third-party TSP risk strategy and implementation.
- g) Ensure appropriate monitoring and management of outsourcing arrangements.
- h) Ensure that a comprehensive inventory of ICT assets and services outsourced or supported by third-party TSPs is established and maintained. This should classify business functions based on their criticality and include an impact assessment of disruptions to the business services supported by third-party TSPs.

4.2 Role of Risk Management Functions

Institutions should integrate the risk management of third-party TSPs in their enterprise-wide risk-management frameworks. They should identify, monitor and manage the risks caused by TSPs to make well-informed decisions on risk management. The role of the risk management function in managing TSPs' risks includes the following: -

- a) Oversee the evaluation and management of risks introduced by third-party TSPs. Institutions may require attestation/assurance reports provided by reputable independent auditors for service providers.
- b) Establish third-party TSPs' risk ownership and management accountability. Assign ownership of assignments related to third-party TSPs to appropriate business lines and/or Information Technology (IT) functions within the institution.
- c) Continuously review and report on risks arising from engagements with third-party TSPs within the institution and other related third-party connections.
- d) Assess the risks and exposures related to third-party TSPs and determine whether they fit within the institution's risk tolerance framework.
- e) Monitor current and emerging risks and changes to laws and regulations.
- f) Maintain a comprehensive third-party TSP risk register.
- g) Reporting third-party TSPs risks consistently and comprehensively to the board to enable timely decision-making and risk prioritization.

4.3 Independent Review and Audit

The review of third-party TSPs requires a collaborative approach that encompasses multiple functions: Internal Audit, Risk Management and External Audit.

4.3.1 Role of Internal Audit

The internal audit function should ensure that:

- a) The TSP policy is correctly and effectively implemented in line with applicable Acts, Regulations, rules and guidelines as well as the institution's broader risk strategy and decisions outlined by the Board and Management.
- b) Assess both the design and effectiveness of the TSP framework implemented.
- c) Review the risk assessment framework for third-party arrangements and ensure that it complies with the institution's risk strategy.
- d) The audit plan and programmes should include a risk-based review of the categorization of outsourced activities, assessing their criticality and materiality to core business operations, service continuity, data integrity, and regulatory compliance.
- e) Report the findings of the assessments to the board.
- f) Establish a formal process for following up on audit findings, including the timely verification and remediation of material audit findings that may have an impact on the proper execution of any third-party TSP arrangements.

4.3.2 Role of External Auditors

External auditors have the following responsibilities:

- a) Obtain an understanding of the institution's dependence on third-party TSPs.
- b) Conduct an independent risk assessment of third-party TSP outsourcing.
- c) Conduct a comprehensive review of the approved third-party TSP strategy and policy.
- d) Report annually to the board and CBK on the findings of the assessments.

4.4 Legal obligations

- 4.4.1 Entering into Third-Party TSP arrangements does not diminish institutions' legal obligations. The board and senior management of the institutions retain the ultimate responsibility for the activities under provided by the third-party service provider including managing third-party risks.
- 4.4.2 Institutions remain responsible for the actions of their third-party TSPs, as well as the fourth and nth parties in the supply chain for related services, and the confidentiality of information pertaining to the customers that is available with the service provider. Therefore, the institutions should retain ultimate control of the third-party TSP activities.

4.5 Internal Controls and Standard of Care

- 4.5.1 Institutions should not engage in third-party TSP arrangements that results in their internal control, business conduct or reputation being compromised or weakened.

- 4.5.2 Institutions must take steps to ensure that the third-party TSPs employ a high standard of care in performing the services as if the activity were not being provided by the third-party.
- 4.5.3 Institutions should also maintain the capability and appropriate level of monitoring and control over third-party TSP arrangements, such that in the event of disruption or unexpected termination of the service, they can continue to conduct business with integrity and competence.

4.4 Third-Party Technology Service Providers Risk Management Lifecycle

Institutions are required to ensure that the Third-Party TSPs Risk Management Lifecycle aligns with the institution's risk appetite and business strategy, with the aim of promoting operational resilience, sound risk governance and regulatory compliance.

The Third-Party TSPs Risk Management Lifecycle encompasses a structured framework for managing risks throughout the entire duration of TSP engagements. This encompasses all processes including TSP selection, contracting, continuous oversight, performance evaluation, and contract termination. The goal of a Third-Party TSPs Life cycle approach is to ensure operational resilience and compliance throughout each process. Each stage is aimed at supporting effective oversight and risk mitigation across the full duration of a TSP relationship. The stages of the lifecycle include:

4.4.1 Identification and Assessment of Critical Services

- (1) Institutions should identify, classify and assess the criticality of proposed TSP services and evaluate the associated risks prior to entering into any arrangement with a TSP.
- (2) A service is considered critical if the failure or disruption of the service would significantly impair the institution's viability, its critical operations or its ability to meet key legal and regulatory obligations. When identifying critical services and their level of criticality, institutions may consider, among other factors, the following:
 - i) Financial/operational reliance on the service.
 - ii) Tolerance for disruption.
 - iii) Sensitivity and regulatory value of shared data.
 - iv) Substitutability of the service.
- (3) Institutions must document and justify the decision to engage a third-party TSP for the provision of critical services.

4.4.2 Pre-Contractual Analysis and Due Diligence

This stage involves conducting an initial risk assessment and due diligence on the third-party TSP prior to formal engagement.

(1) Initial Risk Assessment

- (a) The risk management function should perform a comprehensive risk assessment to evaluate and manage identified potential risks before entering into a TSP arrangement. The risk assessment should, at a minimum, cover the following aspects:
 - i) Financial, technical, operational, and reputational standing of the TSP.
 - ii) Alignment with business strategy and risk appetite.
 - iii) Compatibility with internal control environments.
 - iv) Information security and data protection controls.
 - v) Types of risks presented by the TSP, including strategic, compliance, reputational, ICT/cybersecurity, concentration, and nth-party risk.
 - vi) Compliance with applicable laws and cross-border regulations, including data protection laws.
 - vii) Monitoring and mitigation plans.
 - viii) Business continuity and disaster recovery preparedness.
 - ix) Cloud-specific considerations, including the deployment and service models, and the risks thereof.
- (b) Institutions should weigh the risks of not entering into a third-party relationship against those of proceeding with third-party TSP arrangements.
- (c) Risks may change throughout the life cycle of the TSP arrangement. Accordingly, risk assessments should be continuous, reflecting changes in the risk profile.

(2) Due Diligence

The due diligence stage of the life cycle involves gathering and analysing the information needed to determine how well an arrangement with a specific TSP would support an institution's third-party strategy. Due diligence ensures the TSP is capable of meeting service, security, and compliance expectations. The level of due diligence should be applied proportionately, taking into account the nature, scale and criticality of the service being outsourced. The institution should, at a minimum, consider an assessment of the TSPs:

- i) Operational and technical capabilities.
- ii) Financial capacity and resilience.

- iii) Risk management and internal controls.
- iv) Management of supply chain and geographic risks.
- v) Key personnel and contact points.
- vi) Conflicts of interest and legal exposures.
- vii) Industry experience and alignment with the financial institution's strategy.
- viii) Business continuity and disaster recovery planning.
- ix) Service substitutability and exit feasibility.

4.4.3 Contract Stage

- (1) The contract stage of the life cycle occurs when the terms and conditions of the delivery of services are agreed upon. Contracts must clearly define the nature of the legal relationship between the parties, roles, responsibilities, and safeguards to support risk management and regulatory compliance. The nature and detail of contracts should be appropriate to the institution and the criticality of service. Institutions should ensure that TSP contracts include the following:
- a) The respective rights and obligations of the institutions and the third-party TSP.
 - b) Scope of services, deliverables, performance metrics and Service Level Agreements (SLAs).
 - c) Details of pricing and fee structure.
 - d) Clearly defined subcontracting conditions, including specific requirements governing the subcontracting of critical services. Such provisions should expressly prohibit unauthorized subcontracting. Where subcontracting is permitted, the contractual liability shall at all times remain with the TSP and the institution must ensure that fourth-party risks are effectively managed. Further, subcontracting will require approval by the institution of the use of subcontractors by the third-party TSP for all or part of an outsourced activity.
 - e) Alignment of the contract to the provisions of the Data Protection Act, 2019, including provisions on data ownership, access, confidentiality, and breach notification requirements and liability for such breach for the institution's and customer data.
 - f) Controls to ensure customer data confidentiality and service providers' liability in case of breach of security and leakage of confidential customer related information.
 - g) Enforcement of consumers' rights, such as access to information, fair contractual terms, and corrective actions, in third-party TSP arrangements.
 - h) Where the service provided is customer-facing, customers rights to access of appropriate complaint and redress channels.
 - i) Rights of the Central Bank of Kenya to access, audit, information, and reporting, including audit and inspection rights for the institution and the Central Bank of Kenya.

- j) Rights of the Central Bank of Kenya or persons authorized by it to access the institution's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time.
- k) Right of an institution to conduct audits on the third-party TSP whether by its internal or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the TSP in conjunction with the services performed for the institution.
- l) Compliance by the third-party TSP and nth-party service providers with the institution's cybersecurity standards.
- m) Contingency planning, business continuity, recovery time objectives (RTOs) and recovery point objectives (RPOs).
- n) Intellectual property rights.
- o) Insurance requirements.
- p) Primary and third-party indemnity.
- q) Dispute resolution mechanisms.
- r) Applicable jurisdiction.
- s) Particulars of breach and remedies applicable.
- t) Termination and notification clauses, and minimum periods to execute a termination provision.
- u) Contract period and frequency of renewal, where applicable.
- v) Advance notification of any proposed material changes to the TSPs, including:
 - i) Business strategy or ownership, e.g. mergers, acquisitions.
 - ii) Management or key personnel assigned to the institution's account.
 - iii) Technology infrastructure, architecture, or key nth-party service providers used to deliver the service.
 - iv) Physical location of data centres or offices handling the institution's data.
- w) For TSPs providing critical services, compliance certifications where applicable, and periodic disclosures of audited financial statements to enable institutions assess the TSP's going concern.
- x) Regulatory compliance obligations, including the types of incidents, events, and performance metrics the TSP is required to report. This includes:
 - i) Incident reporting for critical incidents, including security breaches, service disruptions, cybersecurity events, fraudulent activities, control failures, and legal/regulatory actions.
 - ii) For critical services, minimum information to be reported, clearly defined processes for identifying, investigating and remediating incidents related to contracted services and notifying institutions promptly of incidents that impact the TSP's ability to meet contractual obligations.

4.4.4 Onboarding

Institutions should dedicate sufficient resources to support the smooth transition of a new third-party TSP arrangement by:

- a) Addressing due diligence findings.
- b) Familiarizing the TSP with institutions' operations, policies, and systems.
- c) Updating TSP registers and mapping interdependencies. Institutions should maintain a register of all third-party TSP outsourcing arrangements. This register should be included in their risk management framework. The register should, at a minimum, include the following information: -
 - i) A list of all ongoing and previous engagements with TSPs.
 - ii) A unique reference number for each outsourcing arrangement.
 - iii) The duration of the arrangement, including the start date when the contract becomes effective, and the end date.
 - iv) A description of the outsourced function. This should include the nature of data that will be shared between the institution and the third-party TSP.
 - v) The different categories of arrangements as defined by the institution, reflecting the nature of the function to be performed. Institutions should define their own TSP categories and procedures to handle each category.
 - vi) Details on the service provider, i.e. their name, registration details, and contact information.
 - vii) The jurisdiction(s), region(s), and/or country(ies) in which the service is to be performed and where the data required for the service will be processed, stored or hosted, including considerations of cross-border arrangements, data residency requirements, and applicable legal and regulatory obligations.
 - viii) The date of the most recent assessment of the criticality or importance of the outsourced function.

4.4.5 Monitoring

Institutions should, on an ongoing basis, assess and monitor the performance and changes in the risks and criticality of TSP arrangements and report accordingly in line with their governance, risk management framework and strategy. The monitoring process should include:

- a) Review of control effectiveness and SLA compliance.
- b) Escalation process for failures, breaches, or material incidents.
- c) Timely notification of any significant incident by a TSP to the institution.
- d) Risk reassessments following changes or incidents.

- e) Maintenance of updated TSP registers and risk mappings, including changes in their criticality.
- f) Review of the interdependence of critical TSPs for continuous monitoring of concentration risk across the institution.
- g) Performance tracking using Key Performance Indicators (KPIs) and scorecards.
- h) Review of compliance with contracts, regulatory standards, and laws.

4.4.6 Risk Management

(1) As part of their broader risk management framework, institutions should: -

- a) On a continuous basis, identify risks to critical services that may arise from their TSP arrangements.
- b) Implement appropriate and proportionate measures to monitor, manage and mitigate the TSP risks to the delivery of critical services
- c) Assess how a critical third-party TSP understands and assesses its supply chain to identify key nth-party service providers.
- d) Report the outcome of the risk assessments to senior management and boards of directors periodically and as needed according to the institution's policies and procedures. Reporting should include:
 - i) TSP performance summaries.
 - ii) Breaches, incidents, and emerging risks.
 - iii) Portfolio changes and concentration risk.
 - iv) Incident response and remediation tracking.

(2) Concentration Risk Management: -

- a) Institutions must assess and mitigate concentration risks arising from reliance on one or a few TSP providers for critical services.
- b) Diversification of service providers should be pursued where feasible.
- c) Assess and mitigate the risk of critical nth-party relationships and overlapping dependencies which may arise when institutions have both a direct and indirect reliance on the same TSP, where the service provider is both a third-party TSP and an nth-party TSP to other third-party TSPs that the financial institution relies on.
- d) Conduct enhanced due diligence and oversight of third-party TSPs deemed to pose concentration risk during onboarding and ongoing monitoring.

4.4.7 Exit and Transition

(1) The termination stage is where institutions manage planned or unplanned terminations of arrangements. Termination may arise from various circumstances, including:

- a) Expiration or breach of contract.
 - b) The TSP's failure to comply with applicable laws or regulations.
 - c) A strategic decision to seek an alternate TSP, bring the activity in-house or discontinue the activity altogether.
- (2) Institutions should develop exit plans with defined timelines, responsibilities, and resource needs, ensuring business continuity. Exit strategies should be proportionate to the nature, scale and criticality of the service(s) provided. Exit plans should be regularly tested at least once annually for all critical TSP outsourcing arrangements.
- (3) Institutions must manage both planned and unplanned terminations safely and with minimal disruption.
- a) For planned termination(s), institutions should:
 - i) Ensure that transfer of data, systems, and knowledge is structured.
 - ii) Ensure that contracts allow for execution of exit provisions.
 - iii) Ensure that TSPs return or securely destroy all institutional and customer data upon contract termination.
 - b) For unplanned termination(s), institutions should: -
 - i) Maintain contingency plans for abrupt TSP failures.
 - ii) Ensure emergency response teams and budgets are in place.
 - iii) Identify critical services without substitutes and develop internal fallback options.
- (4) The Central Bank may also direct institutions to terminate, suspend, or replace third-party TSPs or TSP arrangements where the arrangement:
- a) Poses a material risk to the safety and soundness of the institution.
 - b) Materially impairs the institution's operational resilience or ability to provide critical services.
 - c) Does not comply with this Guidance or any other applicable law.
 - d) Prevents the Central Bank from exercising its supervisory or inspection powers.
 - e) Exposes customers or the financial system to unacceptable risk.
 - f) Is otherwise contrary to the public interest or financial stability.

4.6 Cybersecurity in Third-Party TSP Arrangements

- a) Institutions shall ensure that they conduct independent cybersecurity testing, including penetration tests, at least once annually.

- b) The independent cybersecurity testing of third-party TSP arrangements shall be included in the scope of the annual independent cybersecurity testing mandated under the Guidance Note on Cybersecurity.
- c) The outcomes of independent cybersecurity testing shall be documented and submitted to the Central Bank of Kenya annually as part of the cybersecurity independent testing.
- d) Any identified weaknesses shall be remediated within defined timelines and subject to follow-up verification by the Central Bank of Kenya.

4.7 Data Protection in Third-Party TSP Arrangements

- a) Institutions shall ensure compliance with the Data Protection Act, 2019, in their engagement with third-party TSPs.
- b) Where the third-party TSP processes personal data on behalf of the financial institution, the parties should enter into appropriate data processing arrangements covering the purpose and scope of processing, confidentiality, security safeguards, data subject rights, breach notification, sub-processing, retention, deletion and cross-border data transfer requirements.
- c) Data confidentiality, integrity, and availability shall always be safeguarded.
- d) Data should comply with requirements for secure access, encryption, and monitoring of data flows, including cross-border transfers.
- e) Institutions shall notify customers of any obligations or requirements to transfer personal data outside the country to third-party TSPs and where possible specify the recipients of customer information.
- f) Institutions should ensure that TSPs are made aware that they are prohibited from unauthorized use, alteration, or disclosure of institutional or customer data.
- g) Institutions should ensure that third-party TSPs adhere to the Data Protection Act, ensuring that they are able to facilitate requests for rectification and erasure of data where applicable.

4.8 AML/CFT/CPF Compliance in Third-Party TSP Arrangements

A financial institution relying on a third-party must:

- a) Enter into an agreement with the third-party outlining the responsibilities of each party;
- b) Retain ultimate responsibility for CDD measures, even where reliance on the third-party is permitted;
- c) Immediately obtain the necessary information concerning the relevant elements of CDD;

- d) Take adequate steps to satisfy itself that copies of identification data and other relevant CDD documentation will be made available by the third-party without delay upon request;
- e) Ensure that the third-party is regulated, supervised or monitored by a competent authority;
- f) Ensure that the third-party has measures in place for compliance with CDD and record-keeping requirements in line with POCAMLA and the Regulations;
- g) Where the third-party is based in another country, assess the money laundering, terrorism financing and proliferation financing risks posed by that country and the adequacy of CDD measures adopted by reporting institutions in that country; and
- h) Where reliance is on a third-party within the same financial group, ensure that group-wide CDD, record-keeping and Anti-Money Laundering, Counter-Financing of Terrorism, and Counter-Proliferation Financing (AML/CFT/CPF) programmes are applied, supervised at group level by a competent authority, and that higher country risk is adequately mitigated by group policies.

4.9 Business Continuity

Institutions should integrate third-party TSP dependencies into business continuity management by: -

- a) Integrating third-party TSP risks into their internal and external Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs).
- b) Periodic testing of BCPs and simulation of disruptions affecting TSPs.
- c) Establishing alternative providers where possible.
- d) Assessing and verifying TSPs' resilience and recovery capabilities.
- e) Joint design and testing of BCPs with third-party TSPs where feasible or utilizing independent parties for such testing.
- f) Ensuring that where alternative TSPs do not exist for critical services, the BCP addresses actions to be taken to ensure the continuity of the service.

4.10 Intragroup Third-Party TSP Arrangements

- a) An institution may outsource a function or service to a parent, subsidiary, affiliate or other entity within the same corporate group or financial conglomerate, provided that the arrangement complies with this Guidance Note.
- b) An intragroup outsourcing arrangement shall be subject to the same governance, risk management, due diligence, contractual, business continuity and oversight requirements applicable to other TSP arrangements, unless otherwise approved by the Central Bank.
- c) An institution may provide critical services to a parent, subsidiary, affiliate or other entity within the same corporate group or financial conglomerate.

- d) An institution acting as an intragroup service provider shall ensure that the services are provided in a safe and sound manner and do not adversely affect its financial condition, operational resilience, regulatory compliance or ability to provide critical services.

4.11 Additional Requirements for Cloud Computing Arrangements

Institutions that enter into a cloud computing TSP arrangement shall comply with this Part in addition to the requirements applicable to third-party technology service provider arrangements.

4.11.1 Cloud Computing Risk Assessment

Before entering into a cloud computing TSP arrangement, institutions shall assess the following aspects.

- a) The suitability of the proposed cloud service model.
- b) The deployment model.
- c) The risks associated with multi-tenancy, virtualisation and shared infrastructure.
- d) Data location and cross-border data transfers.
- e) concentration risk.
- f) Vendor lock-in risk.
- g) The institution's ability to migrate to an alternative provider.

4.11.2 Data Governance

- a) Institutions shall maintain an inventory of data hosted in the cloud and comply with applicable data protection and confidentiality requirements.
- b) Institutions shall identify the jurisdictions in which data is stored, processed and backed up, and ensure that customer and institutional data are protected against unauthorised access, disclosure, alteration or destruction.

4.11.3 Security

- a) Institutions shall ensure that only use cloud services which implement appropriate logical segregation of customer environments.
- b) Institutions shall ensure that data is encrypted in transit and at rest, and that access to cloud resources is restricted to authorised persons.
- c) Further, security logs for cloud computing services should be retained and monitored.

4.11.4 Availability and Operational Resilience

Institutions shall ensure that cloud computing arrangements provide for the following.

- a) Appropriate availability and resilience.
- b) Backup and recovery capabilities.
- c) Disaster recovery arrangements commensurate with the criticality of the service.
- d) Periodic testing of recovery procedures.

4.11.5 Exit Strategy

Institutions shall maintain a documented exit strategy that provides for the following:

- a) The orderly migration of data, systems and services.
- b) Continuity of critical services during migration.
- c) Secure return or destruction of data.
- d) Termination of access by the CSP upon completion of the exit.

4.11.6 Concentration Risk

Institutions shall identify, assess, monitor and manage concentration risk arising from reliance on a single Cloud Service Provider (CSP), reliance on a single geographic region or availability zone, and common dependencies across multiple critical cloud services.

4.11.7 Shared Responsibility

Institutions shall clearly document and periodically review the allocation of responsibilities between the institution and the CSP for the following aspects:

- a) Information security.
- b) Identity and access management.
- c) Encryption and key management.
- d) Backup and recovery.
- e) Logging and monitoring.
- f) Vulnerability management.
- g) Incident response.

PART V: REPORTING

5.1 Institutions shall seek approval of the Central Bank of Kenya of all TSP arrangements for critical TSPs and their proposed TSP arrangements prior to contracting. The

application for approval shall be made in writing and be accompanied by the Third-Party TSP Checklist as specified in **Annex II**.

5.2 Institutions shall provide the Central Bank of Kenya with a register of their third-party TSPs in the format set out in **Annex III (Annual)**.

5.3 Institutions should notify the Central Bank of Kenya within 24 hours of any incident that materially affects service availability, confidentiality, integrity, or incident(s) that could have a significant and adverse impact on the institution's ability to provide adequate services to its customers, its reputation or financial condition in the format set out in **Annex IV (Immediate)** to this Guideline. Material TSP incidents may include: -

- a) **Operational Disruptions:** Major system outages, transaction failures, or service downtime affecting customers.
- b) **Cybersecurity Incidents:** Malware attacks, denial of service, or unauthorized access to critical systems affecting the TSP or the services they provide.
- c) **Data Breaches:** Unauthorized access, exfiltration, or loss of sensitive customer or institutional data hosted or processed by a TSP.
- d) **Fraud and Financial Crime:** Significant cases of fraud, money laundering, or terrorist financing attempts causing financial loss or compromising data privacy for a significant number of customers.
- e) **Third-Party Failures:** Disruptions or breaches from third-party service providers affecting the institution's operations and leading to non-compliance with laws or Central Bank of Kenya directives. The insolvency, bankruptcy, or abrupt termination of services by a critical TSP.
- f) **Contractual Breaches:** Material breaches of the outsourcing agreement by the TSP that could lead to service failure.
- g) **Regulatory Action:** Any major regulatory or legal action taken against a critical TSP in any jurisdiction.
- h) **Other Material Events:** Any incident that may pose reputational, financial, or systemic risk.

5.4 After an incident is resolved, institutions should submit a report as set out in **Annex V**, indicating the cause, origin (internal or third-party), remedial actions, lessons learned and supporting documentation (investigation reports or technical logs).

5.5 On a quarterly basis, institutions shall provide the Central Bank of Kenya with a report in the format set out in **Annex VI (Quarterly)** to this Guideline, concerning its occurrence and handling of third-party TSP incidents via the email address:

fin@centralbank.go.ke.

In the event of any query or clarification, please contact:

The Director
Bank Supervision Department
Central Bank of Kenya
P. O. Box 60000 - 00200
Nairobi
Tel: +254 20 2860000
Email: fin@centralbank.go.ke

DRAFT

REFERENCES

1. Bank for International Settlements. (2024). *Principles for the sound management of third-party risk*. <https://www.bis.org/bcbs/publ/d577.pdf>
2. Central Bank of Kenya. (2025). *Survey on third-party technology service providers in the banking sector*. https://www.centralbank.go.ke/uploads/banking_sector_reports/1558360961_CBK%20Survey%20on%20Third%20Party%20TSPs.pdf
3. Central Bank of Kenya. (2016). *Banking Act*. <https://www.centralbank.go.ke/wp-content/uploads/2016/08/Banking-Act.pdf>
4. Central Bank of Kenya. (2006). *Microfinance Act*. <https://www.centralbank.go.ke/wp-content/uploads/2016/08/MicrofinanceAct.pdf>
5. Central Bank of Kenya. (2013). *Prudential guidelines*. <https://www.centralbank.go.ke/wp-content/uploads/2016/08/PRUDENTIAL-GUIDELINES.pdf>
6. Central Bank of Kenya. (2013). *Risk management guidelines*. <https://www.centralbank.go.ke/wp-content/uploads/2016/08/risk-management-guidelines-january-20131.pdf>
7. Central Bank of Kenya. (2017). *Guidance note on cybersecurity for the banking sector*. <https://www.centralbank.go.ke/wp-content/uploads/2017/09/GUIDANCE-NOTE-ON-CYBERSECURITY-FOR-THE-BANKING-SECTOR.pdf>
8. Financial Stability Board. (2023). *Financial stability implications of third-party dependencies in cloud services*. <https://www.fsb.org/uploads/P041223-1.pdf>
9. Financial Conduct Authority. (2016). *FG16/5: Guidance for firms outsourcing to the 'cloud' and other third-party IT services*. <https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf>
10. European Banking Authority. (2025). *Consultation paper on draft guidelines on sound management of third-party risk*. <https://www.eba.europa.eu/sites/default/files/2025-07/33a0ee15-9601-4c2b-828e-1b09201a6e9f/CP%20on%20Draft%20Guidelines%20on%20sound%20management%20of%20third%20party%20risk.pdf>
11. European Union. (2022). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (Digital Operational Resilience Act – DORA)*. *Official Journal of the European Union*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR>
12. Malta Financial Services Authority. (2020). *Guidance on technology arrangements, ICT and security risk management and outsourcing arrangements*. <https://www.mfsa.mt/wp-content/uploads/2020/12/Guidance-on-Technology-Arrangements-ICT-and-Security-Risk-Management-and-Outsourcing-Arrangements.pdf>

13. Microsoft. (n.d.). *Types of cloud computing*. Microsoft Azure.
<https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/types-of-cloud-computing>
14. Monetary Authority of Singapore. (2021). *Technology risk management guidelines*.
<https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf>
15. Monetary Authority of Singapore. (2026). *Consultation paper on proposed third-party risk management guidelines*. <https://www.mas.gov.sg/-/media/mas-media-library/publications/consultations/bd/2026/consultation-paper---tprmng.pdf>

ANNEX I

High-Level Contents of a Third-Party Technology Service Providers Policy

An institution's Third-Party Technology Service Providers Policy should, at a minimum, include the following: -

- a) The strategic goals, objectives and business needs of the institution in relation to third-party TSPs outsourcing.
- b) The range of activities that may or may not be outsourced to TSPs.
- c) An eligibility criterion for selecting TSPs.
- d) Criteria for identifying critical or material outsourcing.
- e) Procedures for due diligence, approval, and monitoring of TSP engagements.
- f) Risk appetite and tolerance thresholds for outsourcing arrangements.
- g) Due diligence that must be conducted to evaluate whether a particular activity is appropriate for outsourcing. There should be processes for evaluating risks associated with various outsourced activities.
- h) Continuous due diligence that should be conducted on TSPs. This should include the minimum certifications or requirements that TSPs must comply with for the institution to begin an arrangement with them.
- i) Clauses that describe how TSPs should manage subcontracting with other fourth-party or nth party service providers, where applicable.
- j) Business continuity and disaster recovery plans in relation to TSPs, including which business services are outsourced. The business continuity plan should aggregate services based on how critical they are and document potential issues that may arise from a service disruption. Institutions should also introduce contingency plans in case of business disruptions.
- k) Monitoring and mitigation of concentration risk. These are risks arising from outsourcing multiple activities to the same TSPs.
- l) Management of conflict of interest.
- m) Steps that should be taken to ensure compliance with legal and regulatory requirements in the country as well as in other jurisdictions where data may be stored or held by TSPs.

ANNEX II
Third-Party Technology Service Provider Checklist

No.	Section	Description/Question	Yes	No	Responses
1.	Background	Name of Third-Party Technology Service Provider (TSP)			
2.	Criticality of Services	Are the proposed services critical or non-critical?			
3.	Proposed TSP Services	Indicate the proposed services to be supported by TSP.			
4.	Business case	Provide a background and business case on why the institution is proposing the use of the TSP. <i>Attach business case.</i>			
5.	Policy	Does the institution have a Third-Party Technology Service Providers Policy? <i>Attach the policy.</i>			
6.	Governance	Has the Board or relevant Committee of the Board been apprised of and acknowledged the TSP risks presented to them?			
7.	Data governance	Does the institution have a formally defined and board approved data strategy and data governance framework to support data governance in TSP arrangements?			
8.	Due Diligence	Has your institution conducted due diligence on the proposed TSP and TSP arrangement?			

No.	Section	Description/Question	Yes	No	Responses
		Does the due diligence cover the capability, reliability, track record, financial position, and other matters set out in this Guidance? If Yes, please provide details. <i>Attach due diligence report.</i>			
9.	Risk management	Has the institution performed a risk assessment of the TSP arrangement? If Yes, does the risk assessment cover all matters set out in the Guidance Note? <i>Attach risk matrix</i>			
10.	Supply chain risk	Does the risk management and due diligence cover the risks associated with sub-contracting arrangements?			
11.	Risk mitigation	Has the institution considered risk mitigation measures, including triggers to escalate oversight and monitoring when service providers are failing to meet performance, compliance, control or viability expectations? <i>Attach risk matrix</i>			

No.	Section	Description/Question	Yes	No	Responses
12.	Legal and regulatory risk	Are the TSP arrangements contained in a documented draft contract/agreement? If yes, does the agreement address the matters set out in this Guidance Note, particularly Sections 4.43, 4.47, 4.10, and Part V? <i>Attach a copy of the draft agreement.</i>			
13.	Service level agreements	Does the TSP contract contain measurable service level agreements (SLA) and Quality of Service (QoS) requirements and recommended tracking procedure?			
14.	Supply chain management	Does the TSP contract have a provision on supply chain management and the nature of services that can be sub-contracted by the TSP to fourth and n-th parties? If yes, provide details.			
15.	Changes in supply chain	Has a communication mechanism been agreed between the institution and the TSP for changes in material sub-contracting and the rights of the institution in such changes? If yes, provide details.			

No.	Section	Description/Question	Yes	No	Responses
16.	TSP's data privacy policy	Does the TSP have a data privacy policy in compliance with the Data Protection Act, 2019?			
17.	Data classification	Has the institution categorized data according to its sensitivity and privacy, and protection requirements associated with levels of sensitivity?			
18.	Data sovereignty	Outline the jurisdiction where the infrastructure and data will be located or where the service will be provided from.			
19.	Data sovereignty	Has the institution considered the social, political and economic climate of the jurisdiction? If yes, provide details.			
20.	Data sovereignty	Has the institution reviewed and considered the applicable data sovereignty regulations in the jurisdiction where the data will be physically located? If Yes, please provide details.			
21.	VAPT	Has the institution or an independent party performed a Vulnerability Assessment and Penetration Test (VAPT) to determine the security controls in place to			

No.	Section	Description/Question	Yes	No	Responses
		ensure confidentiality, integrity and availability of information such as customer data within the infrastructure of the TSP? If Yes, please attach the VAPT report.			
22.	TSP's cybersecurity measures	Has the institution assessed the TSP's cyber security measures? If yes, provide details.			
23.	Privileged Access Management	Does the service provider have documented policies on privileged user access management? Does this include procedures governing the issuance (including emergency usage and dual control), protection, maintenance and destruction of these accounts? If yes, provide details.			
24.	Business continuity	Does the institution have a documented business continuity plan and disaster recovery plan for the proposed TSP arrangement?			
25.	Backup and recovery	Are there documented data backup and recovery procedures for the institution's data that resides with the TSP? If Yes, do the procedures have defined roles, obligations and			

No.	Section	Description/Question	Yes	No	Responses
		responsibilities of the contracting parties?			
26.	Verification of TSP business continuity and disaster recovery plans	Has the institution verified the TSP's business continuity and disaster recovery plans, including the TSP's ability to recover systems and services within the stipulated recovery time objective (RTO) and recovery point objective (RPO)?			
27.	Incident response	Does the TSP have documented procedures and tools for monitoring, identifying, reporting and responding to cyber security incidents, noncompliance, and performance failure?			
28.	Change management	Is the TSP contract sufficiently flexible to accommodate changes to existing processes and to accommodate new processes in future to meet changing circumstances?			
29.	Change management	Has the TSP provided the institution with the procedure for requesting and effecting changes, including approvals and timelines?			
30.	Access and audit rights	The draft contract should include a provision on audit of the TSP's facilities, systems, processes, and data			

No.	Section	Description/Question	Yes	No	Responses
		relating to the services provided to the institution by the institution, the Central Bank, other regulators and/or their appointed representatives. Does the TSP contract include provisions to allow the Central Bank access, documentation, and information relating to the TSP arrangement? If yes, provide details.			
31.	Oversight of the TSP	Does the TSP contract include reporting mechanisms that ensure adequate oversight of IT security risk management by the service provider? If yes, provide details.			
32.	Exit plan	Does the TSP contract contain exit strategies and clear termination procedures including the situations in which the institution should have the right to terminate the outsourcing agreement?			
33.	Exit plan	Does the TSP contract include a provision on the Central Bank directing termination of the arrangement pursuant to the Guidance Note Section 4.4.7 of this Guidance Note?			
CLOUD COMPUTING					

No.	Section	Description/Question	Yes	No	Responses
34.	CSP, cloud computing service models, and deployment models	Is the service cloud-based? If yes, provide: a) Name of the cloud service provider: b) Service model: c) Deployment model:			
35.	Scope of CSP arrangement	Outline the applications, databases and the nature, description, scope and type of data to be processed and hosted in the cloud.			
36.	Cloud Computing Policy	Does the institution have a cloud computing policy? <i>Attach cloud computing policy</i>			
37.	Concentration risk	Has the institution considered concentration risk that may arise from reliance on a single CSP, reliance on a single geographic region or availability zone, and common dependencies across multiple critical cloud services? If yes, provide details and how this has been mitigated.			
38.	Comingling of data	Is the financial institution's data isolated from other data held by the service provider in			

No.	Section	Description/Question	Yes	No	Responses
		order to avoid commingling of data? If Yes, please provide details.			
39.	Secure removal of data	Are there procedures established to securely destroy or remove data hosted on cloud when the need arises (for example, when the contract terminates)?			
40.	Access monitoring	Are the cloud service provider's access logs monitored? If Yes, please provide details.			
41.	Data sovereignty	Outline the jurisdiction where the cloud infrastructure and data will be located.			
42.	Data sovereignty	Has the institution considered the social, political and economic climate of the jurisdiction? If yes, provide details.			
43.	Data sovereignty	Has the institution reviewed and considered the applicable data sovereignty regulations in the jurisdiction where the data will be physically located? If Yes, please provide details.			

No.	Section	Description/Question	Yes	No	Responses
44.	Data centres	Does the financial institution have a primary and secondary data centre for the cloud services to cater for redundancy? If Yes, provide details including data centre Tiers, availability zones, and region(s).			
45.	Data centre controls	Are there physical and environmental controls at the data centre(s)? If Yes, please provide details.			
46.	Oversight of the CSP	Does the institution have access to adequate and independent resources to appropriately monitor the cloud services and the effectiveness of the controls established by the CSP? If yes, provide details.			

ANNEX III

Third-Party TSPs Register (Annual)

Submit this report on the 5th day after the end of every financial year to the Bank Supervision Department at fin@centralbank.go.ke

[Insert Name of person reporting]

[Quarter]: Year.....

No.	Name of Third-Party TSP	Critical/ Non-Critical Classification	Date of CBK Approval	Services Supported by TSP	Jurisdiction where Service is Performed, where applicable	Jurisdiction where the data is stored or hosted	Last Date of BCP Testing	Last Date of Cybersecurity Testing
1.								
2.								
3.								
4.								
5.								

Signed for and on behalf of

By the duly authorized signatories:

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

ANNEX IV **Third-Party TSP Incident Record (Immediate)**

Third-Party TSP Incident Record (*Immediate*)

[Insert Name of reporting financial institution]

[Insert Date and Time of reporting]: Date..... Time.....

Date of Incident	Time of Incident	Critical Third-Party TSP	Incident Status (Open, Resolved or Closed)	Nature of Incident (Chronological order of events)	Impact Assessment	Actions taken by the time of reporting

Submit the critical third-party TSP incident report within 24 hours after a material incident(s) to the Bank Supervision Department at fin@centralbank.go.ke

Authorised Signatories

Signed for and on behalf of

By the duly authorized signatories:

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

ANNEX V

Third-Party TSP Incident Record (Final)

Third-Party TSP Incident Record (*Upon Resolution*)

[Insert Name of reporting financial institution]

[Insert Date and Time of reporting]: Date..... Time.....

Final Incident Report	
Date and time incident occurred:	
Date and time of resolution:	
Date and time of closure:	
Incident discovery method (how or via which channel was the incident discovered):	
Changes since the previous report (detailed chronological event, stakeholders notified):	
Impact assessment (financial loss amount, assessment on reputational impact based on customer complaints, description of systems affected as well as associated services):	
Incident description (Location, purpose of the system, name of service provider affected where applicable, affected applications /databases/ networks / storage / servers, etc.	
Incident closure (Indicate the root cause of the incident):	
Lessons and remediation:	

Submit the critical third-party TSP incident report within 24 hours after resolution of a third-party TSP material incident to the Bank Supervision Department at fin@centralbank.go.ke

Authorised Signatories

Signed for and on behalf of

By the duly authorized signatories:

Name.....
Designation.....
Contact email address.....
Contact phone number.....
Signature.....

Name.....
Designation.....
Contact email address.....
Contact phone number.....
Signature.....

ANNEX VI **Third-Party TSP Incident Record (Quarterly)**

[Insert Name of reporting financial institution]

[Quarter]..... [Year]

No.	Date of Incident	Time of Incident	Critical Third-Party TSP	Nature of Incident	Action Taken	Time of Resolution	Impact Assessment	Action Taken to Mitigate Future Incidents
1.								
2.								
3.								
4.								
5.								

Submit this report on the 5th day after the end of every quarter to the Bank Supervision Department at fin@centralbank.go.ke

Signed for and on behalf of

By the duly authorized signatories:

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....

Name.....

Designation.....

Contact email address.....

Contact phone number.....

Signature.....