

GUIDELINE ON THIRD-PARTY SERVICE PROVIDERS - CBK/PG/16

CONTENTS

PART I: Preliminary

- 1.1 Title
- 1.2 Authorization
- 1.3 Application
- 1.4 Definitions

PART II: Statement of Policy

- 2.1 Purpose
- 2.2 Scope
- 2.3 Responsibility

PART III: Background

PART IV: Specific Requirements for Third-Party Service Providers

- 4.1 Prohibitions
- 4.2 Legal obligations
- 4.3 Internal Controls and Standard of Care
- 4.4 Customer Rights
- 4.5 Risk Management Practices for Third-Party Service Provider arrangements
- 4.6 Sound Governance Arrangements and Third-Party Risk
- 4.7 Regulatory and Supervisory requirements
- 4.8 Off-shore Third-Party Service Provider arrangements of financial services
- 4.9 Material third-party service provider arrangements outside of Kenya
- 4.10 Use of sub-contractors
- 4.11 Third-Party Service Provider arrangements within a group/conglomerate
- 4.12 Inward Third-Party Service Provider arrangements
- 4.13 Self-assessment of existing/proposed Third-Party Service Provider arrangements
- 4.14 Information to be submitted to Central Bank for approval of Third-Party Service Provider arrangements
- 4.15 Reports to Central Bank

PART V: Remedial Measures and Administrative Sanctions

- 5.1 Remedial Measures and Administrative Sanctions

PART VI: Effective Date

- 6.1 Effective Date

PART I: Preliminary

- 1.1. Title** - Guideline on Third-Party Service Providers.
- 1.2 Authorization** - This Guideline is issued under Section 33(4) of the Banking Act, which empowers the Central Bank of Kenya to issue guidelines to be adhered to by institutions and non-operating holding companies in order to maintain a stable and efficient banking and financial system.
- 1.3 Application** - This Guideline applies to all institutions licensed under the Banking Act (Cap 488) and Non-Operating Holding Companies (NOHCs) who desire to engage Third-Party Service Providers (TPSP). It should be read together with the Risk Management Guideline on Third-Party Risk and Guidance Note on Third-Party Technology Service Providers.
- 1.4 Definitions** - The terms used in this Guideline are as defined in the Banking Act (Cap. 488). Other terms used in this Guideline shall be taken to have the meaning assigned to them hereunder:
- 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 “Critical service”** means a service provided to an institution, the failure or disruption of which could significantly impair an institution’s viability, critical operations, or ability to meet key legal and regulatory compliance obligations.
- 1.4.3 “Critical Third-Party Technology Service Provider”** means a third-party technology service provider who provides a critical service to an institution.
- 1.4.4 “Fourth-Party Service Provider”** means a fourth-party 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.

- 1.4.5 “Key n party”** means an nth party that supports and is essential to the ultimate delivery of a critical service to an institution.
- 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 “Material third-party arrangements”** include arrangements, which if disrupted:
- (a) Have the potential to significantly impact the business operations of the institution or its reputation. They include Critical Third-Party Technology Service Provider arrangements;
 - (b) Pose a risk to the institutions’ safety and soundness;
 - (c) Cast serious doubt on its ability to meet its obligations;
 - (d) May give rise to non-compliance with any regulations;
 - (e) May negatively affect relevant operational resilience and operational continuity requirements; and
 - (f) May potentially impact the profitability of the institution.
- 1.4.8 “Nth-Party Service Provider”** means a service provider that is part of a third-party service provider’s supply chain and supports the ultimate performance of services, activities, functions, processes or tasks directly for an institution.
- 1.4.9 “Outsourcing”** means the use of a third-party service provider (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the institution itself, now or in the future.
- 1.4.10 “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.

1.4.11 “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.

1.4.12 “Third-Party Service Provider” means an entity or individual which performs services, activities, functions, processes or tasks directly for an institution under a Third-Party Service Provider arrangement (which includes but is not limited to “outsourcing”). This includes a Third-Party Technology Service Provider.

1.4.13 “Third-Party Service Provider arrangement” (TPSP arrangement) means a formal arrangement between an institution and a Third-Party Service Provider for the provision of one or more services, activities, functions, processes or tasks to an institution. A Third-Party Service Provider arrangement includes arrangements for the provision of services to an institution by an intragroup service provider. TPSP arrangement excludes:

- Financial services transactions between institutions and their customers, employees or counterparties (e.g. taking deposits from or lending to consumers, or providing or receiving financial market infrastructure (FMI) services, such as clearing or settlement, to other institutions),
- Arrangements between a Third-Party Service Provider and any party in the supply chain (i.e., an nth party to the institution).

1.4.14 “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.

1.4.15 An institution should assess the degree of materiality of the third-party service provider arrangement with third parties. Materiality of the third-party service provider arrangement would be based on:

- a) The level of importance of the activity being provided to the institution;
- b) The potential impact of the Third-Party Service Provider arrangement on the institution on various parameters such as earnings, solvency, liquidity, funding and capital and risk profile;

- c) The likely impact on the institution's reputation and brand value, and ability to achieve its business objectives, strategy and plans, should the third-party service provider fail to perform the service;
- d) The cost of the Third-Party Service Provider arrangement as a proportion of total operating costs of the institution;
- e) The aggregate exposure to that particular Third-Party Service Provider, in cases where the institution outsources various activities to the same TPSP;
- f) The level of criticality of the services;
- g) An activity is considered material if it accounts for at least five percent of the institution's revenue or costs.

PART II: STATEMENT OF POLICY

- 2.1 Purpose** - This guideline is to provide guidance to institutions seeking to enter arrangements with Third-Party Service Providers for the provision of any services on behalf of the institution.
- 2.2 Scope** – This guideline provides a clear guide to institutions on the conditions they must fulfill before, during and on termination of a TPSP arrangement.
- 2.3 Responsibility** – It is the responsibility of an institution proposing to enter into Third-Party Service Provider arrangements, and those that have entered into, any Third-Party Service Provider arrangements to ensure compliance with this Guideline.

PART III: Background

- 3.1** Third-Party Service Provider arrangements can bring cost savings and other benefits. However, they may also increase the risk profile of an institution. Some of the key risks in Third-Party Service Provider arrangements are Strategic Risk, Reputation Risk, Compliance Risk, Operational Risk, Exit Strategy Risk, Counterparty Risk, Country Risk, Third-Party Risks, Contractual Risk, Access Risk, Concentration Risk, Cybersecurity Risk and Systemic Risk. Accordingly, this Guideline should be read together with the Risk Management Guideline on Third-Party Risk and Guidance Note on Third-Party Technology Service Providers.

The failure of a service provider to provide a specified service, a breach in security/confidentiality or non-compliance with legal and regulatory requirements by either the third-party service provider or the institution entering into TPSP

arrangements can lead to financial losses/reputational risk for the institution and could also lead to systemic risks within the entire banking system. An institution entering Third-Party Service Provider arrangements should thus ensure effective management of the potential risks.

Whether activities are performed internally or by a Third-Party Service Provider, institutions are required to operate in a safe and sound manner and in compliance with applicable laws and regulations. While the use of Third-Party Service Providers can reduce institutions' direct control over their activities and assets (including data) and may introduce new risks or increase existing risks, the use of Third-Party Service Provider should neither diminish institutions' responsibility to fulfil their obligations to stakeholders (eg customers, supervisors and other legal authorities) nor impede effective regulatory oversight.

PART IV: SPECIFIC REQUIREMENTS

4.1 Prohibitions

4.1.1 No institution shall engage in material Third-Party Service Providers activities without the prior written approval from the Central Bank of Kenya for such purpose.

4.1.2 Institutions cannot enter into Third-Party Service Provider arrangements for core management functions like:

- Corporate planning decisions (e.g. setting of strategic initiatives, approving business plan, determining risk appetite, capital allocation and resource allocation decisions etc.).
- Organization (e.g. determining governance structure, reporting lines, determining management responsibilities and accountability for business decisions, etc).
- Management and control.
- Decision-making functions like determination of compliance with applicable laws and regulations, decision to grant loans and management of the institutions' investment portfolio, and
- Risk management function.

4.1.3 Institutions will need to notify the Central Bank at least 14 days prior to engaging into Third-Party Service Provider arrangements for these non-material third-party service provider arrangements/ activities.

- Courier services.
- Mail.
- Printing services.
- Credit background checks, background investigations.
- Payroll processing.
- Any other non-material third-party service provider arrangement.
- Any other activity that the Central Bank may specify.

4.1.4 The following are examples of some services that when performed by a Third-Party Service Provider, would be regarded as material and would require prior approval from the Central Bank.

- Information system management and maintenance. These include:
 - Data entry and processing.
 - Data centres.
 - Cloud infrastructure and services including infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), software development.
 - Cyber security services.
 - IT integration services with technology service providers for provision of banking services.
 - Facilities management.
 - End-user support and help desks.
- Application processing (loan originations, credit cards).
- Claims administration (loan negotiations, loan processing, collateral management, and collection of bad debts).
- Employment of contract or temporary staff.
- Business continuity and disaster recovery.
- Marketing and research.
- Cash movement.
- Provision of mobile financial services channels/technology.
- Document processing (e.g. cheques, credit card bill payments, Automated Teller Machine (ATM) switching, Institution statements and corporate payments).
- Professional services related to business activities of institution e.g. accounting, internal audit and secretarial services.
- Security document printing and processing e.g. cheque Printing, card processing.

- Customer-facing digital banking platforms.
- Legal function services.
- Certified Secretary services.
- Performance of Know Your Customer, (KYC) and Customer Due Diligence (CDD) measures related to Anti-Money Laundering compliance.
- And any other activity the Central Bank may specify.

4.1.5 The following Third-Party Service Provider arrangements will not require Central Bank notification or approval

- Use of common network infrastructure such as Visa/MasterCard.
- Normal maintenance contracts for IT systems.
- Market information services such as Bloomberg, Moody's, Standard and Poor.
- Clearing and settlement arrangements between institutions.
- Correspondent banking services.
- Credit reference bureau services.
- Professional advisory services e.g. legal opinions, legal representations, conveyancing, valuations. financial markets infrastructures (FMIs") (e.g., clearing houses, trade repositories, central securities depositories, systemically important payment systems and SWIFT messaging network) and utilities (e.g., telecommunications and electricity providers).
- Services that are not for the conduct of any financial business of the institution and where the service provider does not receive, handle or have access to institution's confidential information or customer information (e.g., cleaning, gardening and pantry services, including the maintenance of vending machines).
- Any other activity the Central Bank may specify.

4.1.6 Creating and maintaining a register of third-party service provider arrangements

- Institutions should keep a record of third-party service provider arrangements and update the record when there are new arrangements or when existing arrangements change in ways that may affect risk.

- Institutions will be required to submit an updated register of third-party arrangements to the Central Bank by January 5th of every year and/ or upon request. This register needs to minimally include all the institution's material third-party arrangements (which include material sub-contractors).

4.2 Legal Obligations

- 4.2.1 Entering into Third-Party Service Provider arrangements by an institution does not diminish its legal obligations. The board and senior management of the institutions retain the ultimate responsibility for the activities being provided by the third-party service provider including managing third-party risks.
- 4.2.2 Institutions remain responsible for the actions of third-party service providers 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 service providers activities.
- 4.2.3 When an institution is performing due diligence in relation to third-party service provider arrangements, it is imperative to consider all relevant laws, regulations, guidelines and conditions of approval, licensing or registration.

4.3 Internal Controls and Standard of Care

- 4.3.1 An institution should not engage in third-party service provider arrangements that result in its internal control, business conduct or reputation being compromised or weakened.
- 4.3.2 An institution has to take steps to ensure that the third-party service providers employ a high standard of care in performing the services as if the activity were not being provided by the third-party.
- 4.3.3 The institution also needs to maintain the capability and appropriate level of monitoring and control over third-party service provider arrangements, such that in the event of disruption or unexpected termination of the service, it remains able to conduct its business with integrity and competence.

4.4 Customer Rights

- 4.4.1 Third-party service provider arrangements should not affect the rights of a customer against the institution, including the ability of the customer to obtain redress as applicable under relevant laws including the Data Protection Act for any data breaches.
- 4.4.2 Where the customers are required to deal with the service providers in the process of dealing with the institution, the institution must reveal to their customers in the product brochures/agreements the role of the third-party service provider and nth providers and their obligations towards the customers.

4.5 Risk Management Practices for Third-Party Service Provider arrangements

4.5.1 Third-Party Risk Management Framework

- 4.5.1.1 Institutions should establish a third-party risk management framework (TPRMF) aligned with its overall operational risk approach, covering identification, assessment, monitoring, reporting, and controls. Further guidance on this is provided in the Risk Management Guideline on Third-Party Risk issued by the Central Bank.
- 4.5.1.2 Institutions should also maintain alongside this framework, a risk management strategy aligned with its overall risk appetite and other key strategies. This strategy should define when third-party service provider arrangements should be entered into, standards for evaluating risks and benefits of these arrangements, implications of such arrangements on the institution's safety and soundness, what are the acceptable levels of risk and disruption, and when the institution should exit an arrangement.
- 4.5.1.3 The institution should ensure it has competent and adequate staff to monitor and manage the risks posed by third-party arrangements.

4.5.2 Role of the Board

- 4.5.2.1 The institution's governance, risk management, and strategy form the foundation for managing third-party risks across all stages of the Third-Party Service Providers arrangement. The board of directors has ultimate

responsibility for the oversight of the institution's third-party risks and should approve a clear strategy, policies and define the institution's risk appetite and associated tolerance for disruption.

- 4.5.2.2 Ensure that senior management implements policies and processes of the third-party risk management framework (TPRMF) in line with the institution's third-party strategy, including reporting of third-party service provider (TPSP) performance and risks related to TPSP arrangements, and mitigating actions to the board of directors.
- 4.5.2.3 The board of directors should hold senior management accountable for the TPRMF's implementation.
- 4.5.2.4 The Board and Senior Management of an institution retain ultimate responsibility for effective management of risks arising from Third-Party Service Provider arrangements. While an institution may delegate its day-to-day operational duties to the service provider, the responsibilities for effective due diligence, oversight and management of Third-Party Service Provider arrangements and accountability for all Third-Party Service Provider arrangements decisions, continue to rest with the institution, its board and senior management. The board or a committee delegated by it is responsible for:
 - a) Approving a framework to evaluate the risks and materiality of all existing and prospective Third-Party Service Provider arrangements and the policies that apply to such arrangements;
 - b) Laying down appropriate approval authorities for Third-Party Service Provider arrangements depending on risks and materiality;
 - c) Undertaking regular review of Third-Party Service Provider arrangements and strategies for their continued relevance, safety and soundness;
 - d) Deciding on business activities of a material nature to be provided by Third Party Service Providers, and approving such arrangements; Establishing a comprehensive Third-Party Service Provider arrangements risk management programme to address third party arrangements and the relationship with the service providers;
 - e) Assessing how the Third-Party Service Provider arrangements will support the institutions' objectives and strategic plan; and

- f) Assessing management competencies for developing sound and responsive Third-Party Service Provider arrangements management policies and procedures as commensurate with the nature, scope and complexity of the arrangements.

4.5.2.5 The board of directors should approve a Third-Party Service Provider arrangements strategy. It should be consistent with other relevant strategies and the institution's risk appetite. It should cover the following:

- a) whether and the extent to which the institution should enter into Third-Party Service Provider arrangements;
- b) the services that should or should not be performed by a Third-Party Service Provider;
- c) standards for the ongoing evaluation of risks, costs and benefits associated with reliance on one or more Third-Party Service Provider; and
- d) the conditions, if any, that should trigger an exit from Third-Party Service Provider arrangements.

4.5.3 Role of Senior Management

Senior management of an institution is responsible for the following as related to Third-Party Service Provider arrangements.:

- a) Senior management should ensure communication of the institution's third-party strategy and policy to all relevant stakeholders, including its personnel and intragroup entities.
- b) Ensuring that roles and responsibilities of all staff are appropriately defined, including those related to Third-Party Service Provider arrangements and based on risk and complexity, establish a central function to monitor all Third-Party Service Provider arrangements;
- c) Evaluating the risks and materiality of all existing and prospective Third-Party Service Provider arrangements, based on the framework approved by the board;
- d) Developing and implementing sound and prudent Third-Party Service Provider arrangements, policies and procedures that include clearly defined roles and responsibilities to manage TPSP arrangements commensurate with their nature, scope and complexity;
- e) Reviewing periodically the effectiveness of policies and procedures;

- f) Communicating information pertaining to material Third-Party Service Provider arrangements risks to the board in a timely manner;
- g) Ensuring that contingency plans, including availability of alternative service providers, based on realistic and probable disruptive scenarios, are in place and tested;
- h) Undertaking periodic review of Third-Party Service Provider arrangements. arrangements to identify new material outsourcing risks as they arise;
- i) Ensuring that there is independent review and audit for compliance with set policies regarding Third-Party Service Provider arrangements.
- j) Ensuring that the internal audit function has the authority to
- k) assess and audit any outsourced functions; and
- l) Ensuring that regulatory requirements on Third-Party Service Provider arrangements are complied with at all times.

4.5.4 Risk assessment

- 4.5.4.1 An institution should identify and assess the types and levels of risks, and the materiality of potential services provided through a third-party service provider arrangements.
- 4.5.4.2 Assessment of risks should be done when the institution is planning to enter into a third-party arrangement, and also when there are major changes impacting the arrangement.
- 4.5.4.3 Based on the risk assessment results, institutions should:
 - i) assess the adequacy of their current control environment to incorporate Third-Party Service Provider arrangements;
 - ii) plan appropriate risk monitoring, reporting and escalation;
 - iii) plan mitigation measures;
 - iv) communicate expectations of the proposed Third-Party Service Provider arrangement to stakeholders; and
 - v) develop related proposed contractual terms and conditions.

4.5.5 Third-Party Service Provider Policy

- i) An institution intending to enter into Third-Party Service Provider arrangements for any of its financial activities should put in place a comprehensive Third-Party Service Provider policy, approved by its Board, which incorporates, inter -alia;

- a) strategic goals, objectives and business needs of an institution in relation to Third-Party Service Provider arrangements;
- b) clear definition of the range of activities that may be sought from Third-Party Service Providers and those core activities which cannot be sought;
- c) steps that should be taken in evaluating whether a particular activity is appropriate for Third-Party Service Provider arrangements
- d) criteria for determining material Third-Party Service Provider arrangements.
- e) processes for evaluating risks associated with Third-Party Service Provider arrangements;
- f) criteria for evaluating Third-Party Service Provider relationships including necessary controls and reporting processes on an ongoing basis;
- g) eligibility criteria for selecting third-party service providers taking into account any relation, directly or indirectly, with the latter;
- h) issues addressing risk concentrations and risks arising from contracting multiple activities to the same Third-Party Service Provider;
- i) steps that should be taken to ensure compliance with legal and regulatory requirements in both home and host countries;
- j) contingency plan in case of business disruptions;
- k) roles and responsibilities of all stakeholders, materiality assessment criteria, vendor management, risk assessment and mitigation for risks associated with Third-Party Service Provider arrangements including contingency plan and exit strategy; and
- l) responsible unit or individual(s) responsible for monitoring and managing the Third-Party Service Provider arrangements.

4.5.6 Evaluating the Capability of the Third-Party Service Provider

- 4.5.6.1 In considering or renewing a Third-Party Service Provider arrangement, appropriate due diligence should be performed to assess the capability of the Third-Party Service Provider to comply with obligations in the TPSP agreement.
- 4.5.6.2 Due diligence should take into consideration qualitative and quantitative, financial, operational and reputational factors.

- 4.5.6.3 Institutions should consider whether the Third-Party Service Provider systems are compatible with their own and also whether their standards of performance including customer service are acceptable.
- 4.5.6.4 Where possible, institutions should obtain independent reviews and market feedback on the third-party service provider to supplement their own due diligence findings.
- 4.5.6.5 The due diligence should involve an evaluation of all available information about the third-party service provider, including but not limited to:-
- a) Past experience and competence to implement and support the proposed activity over the contracted period;
 - b) Financial soundness, technical capabilities and ability to service commitments even under adverse conditions;
 - c) Business reputation and culture, compliance, complaints and outstanding or potential litigation;
 - d) Security and internal control, audit coverage, reporting and monitoring environment and business continuity management;
 - e) External factors like political, economic, social and legal environment of the jurisdiction in which the third-party service provider operates and other events that may impact service performance.
 - f) Ensuring due diligence by third-party service provider of its employees.
 - g) Ensuring that potential conflicts of interest are addressed in case service provider is a related/affiliated party, or where it provides similar services to competitors. Institutions shall also identify all potential and actual conflicts to ensure that such are avoided.
- 4.5.6.6 Due diligence undertaken during the initial evaluation process should be documented and re-performed periodically as part of the monitoring and control processes of Third-Party Service Provider arrangements.
- 4.5.6.7 The due diligence process can vary depending on the nature of the TPSP arrangement. For instance, reduced due diligence may be sufficient where no developments or changes have arisen to affect an existing Third-Party Service Provider arrangement or where the Third-Party Service Provider arrangements is to a member of the group.
- 4.5.6.8 An institution should ensure that the information used for due diligence evaluation is current and should not be more than 12 months old.

- 4.5.6.9 Institutions should at least on annual basis review the financial and operational conditions of the third-party service provider to assess the ability to meet its obligations. Such due diligence should highlight any deterioration or breach in standards, confidentiality, security or business continuity preparedness.
- 4.5.6.10 Institutions should retain the ability to maintain business continuity plans (BCPs), disaster recovery plans (DRPs) and other relevant plans (e.g. crisis communication plans) consistent with or benchmarked to the institution's tolerance for disruption of critical services.
- 4.5.6.11 Institutions should consider the availability of potential alternative Third-Party Service Providers and assessment of related risks;
- 4.5.6.12 Institutions should determine whether the arrangement under consideration may result in unacceptable institution-level concentration risk; and
- 4.5.6.13 Institutions should consider how responsibility for security, resilience and technical configurations will be shared between the institution and Third Party Service Provider with respect to the delivery of services and the associated risks;

4.5.7 Third-Party Service Provider Agreement

- 4.5.7.1 TPSP arrangements should be governed by a clearly written contract, the nature and detail of which should be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the regulated entity.
- 4.5.7.2 A written contract is an important management tool and appropriate contractual provisions can reduce the risk of non-performance or disagreements regarding the scope, nature and quality of the service to be provided.
- 4.5.7.3 The terms and conditions governing the contract between the institution and the TPSP should be carefully defined in written agreements and vetted by a competent authority on their legal effect and enforceability.
- 4.5.7.4 Every TPSP arrangement agreement should address the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages.
- 4.5.7.5 The agreement should be sufficiently flexible to allow the institution to retain an appropriate level of control over the TPSP arrangement and the right to intervene with appropriate measures to meet legal and regulatory obligations.

- 4.5.7.6 The agreement should also bring out the nature of legal relationship between the parties, that is, whether agent–principal or otherwise. Some of the key provisions of the contract include:
- a) The contract should clearly define what activities are going to be provided including appropriate service and performance standards along with the timeframe for implementation.
 - b) The institution must ensure it has the ability to access all books, records and information relevant to the TPSP arrangements.
 - c) The contract should provide for continuous monitoring and assessment by the institution of the TPSP so that any necessary corrective measure can be taken immediately.
 - d) A termination, exit clause and minimum periods to execute a termination provision, if deemed necessary, should be included.
 - e) Controls to ensure customer data confidentiality and TPSP arrangements liability in case of breach of security and leakage of confidential customer related information.
 - f) Contingency plans to ensure business continuity.
 - g) The contract should provide for the approval by the institution of the use of subcontractors by the TPSP for all or part of a TPSP arrangement.
 - h) Provide the institution with the right to conduct audits, on the TPSP 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 TPSP in conjunction with the services performed for the institution.
 - i) A clause to allow the Central Bank 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. The agreement should further provide that in the event these are not made accessible to the Central Bank within a reasonable time, the Central Bank may pursue any or all of the remedial actions and administrative sanctions provided for under the Banking Act.
 - j) A clause to recognize the right of the Central Bank to cause an inspection to be made of a service provider of an institution and its books and account by one or more of its officers or employees or other persons.
 - k) There should be dispute resolution mechanism between parties involved in TPSP arrangement.

- l) Details of pricing and fee structure of TPSP contract should be provided.
- m) Clause clearly stipulating the deliverables and obligations of the parties in the contract.
- n) Clause that addresses the service provider's responsibility for data confidentiality and security of both the institution and its customers from intentional or inadvertent disclosure to unauthorized persons.
- o) The respective rights and obligations of the institutions and the third-party service provider.
- p) A penalty clause in the event that the third-party service provider fails to provide services as mutually agreed.
- q) Provide for continuous monitoring and assessment of the service provider's performance so that any necessary corrective measures can be taken promptly.
- r) Contracts should reflect the right of institutions to obtain information (including incident notifications) about key nth parties on an ongoing basis.

In entering into the agreement, the institutions shall ensure that no TPSP arrangement is made with the third-party service providers having close relationship with the management or employees of the institutions, which may create a conflict of interest.

4.5.8 Monitoring and Control of Third-Party Service Provider Activities

- 4.5.8.1 The institution should have in place a management structure to monitor and control its Third-Party Service Provider arrangements. Such a structure will vary depending on the nature, scope and complexity of the Third-Party Service Provider arrangements.
- 4.5.8.2 As TPSP arrangement relationships and interdependence increase in materiality and complexity, a more rigorous risk management approach should be adopted. An institution also has to be more proactive in its relationship with the Third-Party Service Provider.
- 4.5.8.3 A TPSP arrangement which was previously not material may subsequently become material from incremental activities undertaken by the same Third-Party Service Provider on behalf of the institution or an increase in volume or nature of the activity by the Third-Party Service Provider. Material Third-Party Service Provider risks may also

arise when the third party is undertaking material activities or plans to sub-contract the service or makes significant changes to its sub-contracting arrangements.

4.5.8.4 The institution should ensure that TPSP arrangements with the service providers contain provisions to address their monitoring and control of outsourced activities.

4.5.8.5 A structure for effective monitoring and control of material Third-Party Service Provider arrangements would at a minimum comprise the following:

- a) A central record of all material Third-Party Service Provider arrangements that is readily accessible for review by the board and senior management of the institution should be maintained. The records should be updated promptly and form part of the corporate governance reviews undertaken by the board and senior management of the institution.
- b) Regular audits by either the internal auditors or external auditors of the institution should assess the adequacy of the risk management practices adopted in overseeing and managing the Third-Party Service Provider arrangement, the institution's compliance with its risk management framework and the requirements of these guidelines.
- c) Institutions should at least on an annual basis, review the financial and operational condition of the service provider to assess its ability to continue to meet its TPSP arrangement/outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider should highlight any deterioration or breach in performance standards, confidentiality and security, and in business continuity preparedness.

Commented [EK1]: How does this tie in to the earlier introduction of a register to be maintained by institution?

4.5.9 Termination

4.5.9.1 Institutions need to terminate the arrangement in a safe and sound manner.

4.5.9.2 Exit plans need to cater for different plausible termination scenarios, and be regularly updated and tested. The level of detail in these plans should vary in accordance with the materiality and substitutability of the services provided.

- 4.5.9.3 Central Bank may also direct the institution to terminate third -party service provider arrangements in case the TPSP or institution or nth party breaches any of the provisions in this Guideline.
- 4.5.9.4 Institutions should immediately report to Central Bank termination of any TPSP arrangement.

4.5.10 Confidentiality and Security

An institution should satisfy itself that the Third-Party Service Provider's security policies, procedures and controls will enable it to protect confidentiality and security of the customer information. An institution should take the following steps as minimum to ensure that customer confidentiality is addressed: -

- a) Access to customer information by staff of the Third-Party Service Provider arrangements should be limited to those areas where the information is required in order to perform the TPSP arrangement.
- b) The institution should ensure that the Third-Party Service Provider arrangements are able to isolate and clearly identify the institution's customer information, documents, records and assets to protect the confidentiality of the information.
- c) The institution should review and monitor the security practices and control processes of the service provider on a regular basis and require the Third-Party Service Provider to disclose security breaches.
- d) The institution should immediately notify CBK in the event of any breach of security and leakage of confidential customer-related information. In these eventualities, the institution would be liable to its customers for any damage.
- e) Ensure that the service provider has put in place mechanisms to protect customer data as per the requirements of the Data Protection Act.
- f) Where the TPSP qualifies as a data processor, ensure that they have obtained the necessary registration from the Office of the Data Protection Commissioner (ODPC).
- g) Where there is integration between the institution and the Third-Party Service Providers, Information and Communication technology (ICT) systems, an Information Systems Security assessment should be undertaken.

- h) The institutions that engage in Third-Party Service Provider arrangements should take appropriate steps to protect confidential information.
- i) The institutions should prohibit TPSPs from disclosing customer information to any party except for regulatory purpose or as required by law.
- j) The institutions, before providing data to third-party service providers, shall ensure that proposed TPSP arrangement complies with the relevant statutory/regulatory requirements related to confidentiality of its customers.
- k) Depending on the nature of the Third-Party Service Provider arrangement, the institutions should consider obtaining customer consent where customer data may be transmitted to a TPSP as part of their contractual arrangement with the customers.
- l) In cases where TPSP arrangements involve disclosure of confidential customer information to service provider, the institutions shall seek consent of the customer and notify the Central Bank accordingly.
- m) The institution must ensure that Third-Party Service Provider arrangement does not violate any statutory/regulatory requirements.
- n) Ensure that the Third-Party Service Provider arrangement does not hinder ability of the institution to provide timely data and other information to Central Bank.

4.5.11 Business Continuity Management and Disaster Recovery

An institution should ensure that its business continuity preparedness is not compromised by TPSP arrangements. The institution should take steps to evaluate and satisfy itself that the interdependency risk arising from the Third-Party Service Provider arrangement can be adequately mitigated such that the institution remains able to conduct its business with integrity and competence in the event of disruption, or unexpected termination of the Third-Party Service Provider arrangement or liquidation of the TPSP. The steps to ensure business continuity in Third-Party Service Provider arrangements include:-

- a) The institution requiring its Third-Party Service Providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. Institutions should ensure that Third-Party Service Providers periodically test their Business

Continuity and Recovery Plans. Institutions should also consider joint testing and recovery exercises with their TPSPs.

- b) In order to mitigate the risk of unexpected termination of the Third-Party Service Provider arrangement or liquidation of the Third-Party Service Provider, institutions should retain an appropriate level of control over their Third-Party Service Provider arrangements including the right to intervene to safeguard business operations.
- c) In establishing a viable contingency plan, institutions should consider the availability of alternative Third-Party Service Provider and hand-over process to a new acceptable supplier or the possibility of bringing the TPSP arrangements back in-house in an emergency and the costs, time and resources that would be involved.
- d) TPSP arrangements often leads to the sharing of facilities operated by the Third-Party Service Provider. The institution should ensure that Third-Party Service Providers are able to isolate the institution's information, documents and records, and other assets. Under adverse conditions, the institution should ensure that all documents, records of transactions and information, can be removed from the possession of the third-party service provider in order to continue its business operations, or be deleted, destroyed or rendered unusable.

4.6 Sound Governance Arrangements and Third-Party Risk

4.6.1 Sound Governance Arrangements and TPSP arrangements

Third-Party Service Provider arrangement shall not result in the delegation by the senior management of its responsibility. The Board of Directors of the institution shall at all times remain fully responsible and accountable for:

- i. ensuring that the institution meets on an ongoing basis the conditions with which it must comply to remain licensed, including any conditions which may be imposed by the Central Bank;
- ii. the internal organization of the institution;
- iii. the identification, assessment and management of conflicts of interest;
- iv. the setting of the institution's strategies and policies (e.g. the business model, the risk appetite, the risk management framework);
- v. overseeing day-to-day management of the institution including the management of all risks; associated with Third-Party Service Provider arrangements; and

- vi. the oversight and monitoring of management decision-making.

4.7 Regulatory and supervisory requirements

- 4.7.1 An institution should not enter into any TPSP arrangement of a material function before getting approval from Central Bank.
- 4.7.2 Proposals to enter into material functions must be submitted to Central Bank in writing well in advance of the date on which it is intended that the TPSP arrangement will commence.
- 4.7.3 An institution that has entered into or is planning material Third-Party Service Provider arrangement, or is planning to vary any such TPSP arrangements, should notify Central Bank.
- 4.7.4 The degree of detail of the proposal will depend on the functions that the institution proposes to enter into Third-Party Service Provider arrangements and the service provider to be used. The proposal should include details of:
 - i. the rationale for the third-party service provider arrangement;
 - ii. details relating to the proposed service provider;
 - iii. risk matrix identifying potential risks and how they will be mitigated;
 - iv. draft third-party service provider arrangement agreement between the parties involved; and
 - v. a description of the methods that the institution will employ to ensure that it retains its ability to control and monitor the third-party service provider arrangement.
- 4.7.5 TPSP arrangement, whether the service provider is located in Kenya or abroad should not impede or interfere with the ability of the Central Bank to effectively oversee and manage its activities or impede the Central Bank in carrying out its regulatory and supervisory functions.

4.8 Off-shore Third-Party Service Provider arrangements of financial services

Commented [EK2]: Renumber appropriately

- 4.8.1 The engagement of service providers in a foreign country exposes an institution to country risks including economic, social and political conditions and events in a foreign country that may adversely affect the institution. These conditions and events could prevent the service provider from carrying out the terms of the TPSP agreement with the institution.

- 4.8.2 Institutions that engage in cross-border Third-Party Service Provider arrangements should take into account country risk and their capacity to control the third-party service provider to deliver the service uninterruptedly.
- 4.8.3 Institutions should also consider scenarios in case of disruptions in business continuity. An aspect that institutions should consider seriously in this respect is how quickly and efficiently the processes could be reverted to the home country so as to keep at minimum any potential disruption of service by the institution due to this factor.
- 4.8.4 To manage the country risk involved in off-shore Third-Party Service Provider arrangements, the institution should take into account and closely monitor government policies as well as political, social, economic and legal conditions in countries where the service provider is based, during the risk assessment process and on a continuous basis, and establish sound procedures for dealing with country risk problems. This includes having appropriate contingency and exit strategies.
- 4.8.5 Off-shore Third-Party Service Provider arrangements should only be entered into with parties operating in jurisdictions generally upholding confidentiality clauses and agreements. The governing law of the arrangement should also be clearly specified.
- 4.8.6 The TPSP arrangements outside Kenya should be conducted in a manner so as not to hinder efforts to supervise or reconstruct the Kenyan activities of the institution in a timely manner. Specifically, an institution should not outsource to jurisdictions where unfettered access to information by CBK or its authorized person, and the internal and external auditors of the institution, may be impeded by legal or administrative restrictions. CBK may communicate directly with the home or host regulator of the institution or the service provider, as the case may be, to seek confirmation relating to these matters.
- 4.8.7 An institution should seek CBK authority if any overseas authority were to seek access to its customer information.

4.9 Material third-party service provider arrangements outside of Kenya

These arrangements should be conducted in a manner so as not to hinder Central Bank's efforts to supervise the Kenyan business activities of the institution. In

particular, institutions should not enter into third-party arrangements in jurisdictions where there are legal or administrative restrictions that prevent Central Bank or its agents from prompt access to information. Additionally, institutions should notify Central Bank if any overseas authority were to seek access to its customer information or if a situation were to arise where the rights of access of the institution and Central Bank have been restricted or denied.

4.10 Use of sub-contractors

For material third-party service provider arrangements, even where third-party service provider engages a sub-contractor to perform the material third-party services, the same requirements under this Guideline and the Risk Management Guideline on Third-Party Risk and Guidance Note on Third-Party Technology Service Providers apply.

Before the service provider engages the sub-contractor, the service provider is to notify the institution in writing. The institution is then to conduct a risk assessment to satisfy itself that the sub-contracting will not pose any risks to the institution.

Institutions should then take reasonable steps to ensure that material sub-contractors are held to similar standards as material third-party service providers.

4.11 Third-Party Service Provider arrangements within a group/conglomerate

The risk management practices expected to be adopted by an institution while engaging in Third-Party Service Provider arrangements to a related party (i.e. a party within the Group/ Conglomerate) would be identical to those specified in this guideline. In addition, before entering into Third-Party Service Provider arrangements to the group:

- i) The engaging institution should demonstrate that it can manage the risk involved.
- ii) The engaging institution should be a member of a group that is subject to supervision on a consolidated basis in conformity with Basel Core Principles for Effective Banking Supervision¹.

For Third-Party Service Provider arrangements within the group/ conglomerate an institution should ensure that:-

- i) The Board of Directors is ultimately responsible for the arrangement and must establish policies and procedures before contracting intra-group services.

¹ <https://www.bis.org/bcbs/publ/d573.pdf>

- ii) Transactions between the group/ conglomerate service provider must be conducted on an arm's length basis.
- iii) There is a clearly defined Service Level Agreement (SLA) in compliance with the requirements of Section.4.5.7 of this Guideline.
- iv) Performance metrics, roles, responsibilities and dispute resolution mechanisms for the third-party service provider arrangement have been outlined.
- v) Third-Party Service Provider maintains information security, risk management, and service delivery standards as required by Central Bank.
- vi) The institution has in place contingency plans, and a viable exit strategy, in case the group company is unable to continue with the third-party service provider arrangement.
- vii) There is compliance with all the requirements of this Guideline.

4.12 Inward Third-Party Service Provider arrangements

For inward Third-Party Service Provider arrangements of material activities, an institution shall seek approval from the Central Bank. It shall detail the particulars of the services to be provided and furnish the following information:

- i) The functions to be performed by the service provider (local institution) should be detailed in the Third-Party Service Provider agreement. The outsourcer remains ultimately responsible for the Third-Party Service Provider agreement.
- ii) The copies of the Third-Party Service Provider agreement between the institution and foreign entity should be made available to Central Bank. The Third-Party Service Provider agreement should address all the requirements in clause 4.5.7 of this Guideline including the Data Protection Act.
- iii) Risk matrix of the proposed arrangement identifying risks and mitigants.
- iv) Approval from the host regulator of the foreign entity for the proposed outsourcing arrangement.

4.13 Self-assessment of existing/proposed Third-Party Service Provider arrangements

Institutions are expected to conduct a self-assessment of their existing/proposed Third-Party Service Provider arrangements, in the light of this guideline and rectify deficiencies/shortcomings if any observed in this regard.

4.14 Information to be Submitted to Central Bank for approval of Third-Party Service Provider Arrangements

In seeking the approval of the Central Bank for a Third-Party Service Provider arrangement and in order to process the request, institutions are required to submit the following documents/information:

- i. TPSP arrangement policy;
- ii. Description on the rationale for entering into Third -Party Service Provider arrangement;
- iii. Profile of the Third-Party Service Provider;
- iv. Due diligence report on the Third-Party Service Provider;
- v. TPSP agreement to be entered between the institution and the Third-Party Service Provider;
- vi. Business continuity, disaster recovery and contingency plan for the Third-Party Service Provider arrangement;
- vii. Workflow or data flow diagram for provision of the TPSP services;
- viii. Information systems security assessment report for the provision of the services;
- ix. Registration certificates from the Office of the Data Protection Commissioner (ODPC);
- x. Risk assessment matrix performed on the Third-Party Service Provider arrangement, including all identified risks and mitigants put in place by the institution;
- xi. Assurance that all the internal control procedures and risk management systems are in place for the implementation of the Third-Party Service Provider arrangement;
- xii. Data protection policies by the institution and the Third-Party Service Provider data protection framework; and
- xiii. Any other relevant information as may be required by the Central Bank.

4.15 Reports to Central Bank

All institutions will report to the Central Bank on an annual basis the activities they have entered into Third-Party Service Provider arrangements. This report should be received by CBK by 5th January of every year. The report should detail the type of TPSP arrangements and the date the TPSP arrangement commenced. The report should also include materiality classification, date of notification or approval by Central Bank, concentration risk indicators, country risk exposure and cloud and Information and Communications Technology (ICT) Third-Party Service Provider arrangement disclosures where applicable.

PART V: REMEDIAL MEASURES AND ADMINISTRATIVE SANCTIONS

5.1 Remedial measures

Where any provision of this Guideline is breached or not observed, the Central Bank may pursue any or all of the remedial actions and administrative sanctions provided for under the Banking Act.

PART VI: EFFECTIVE DATE

6.1 Effective Date - The effective date of this Guideline shall be 1st January 2027.

ENQUIRIES

Enquiries on any aspect of this guideline should be referred to:

The Director
Bank Supervision Department
Central Bank of Kenya
P. O. Box 60000 - 00200

NAIROBI

TEL.2860000 e-mail: fin@centralbank.go.ke