



CREDENCE AFRICA
EXPERTISE. DELIVERED

Date: 26th May 2025

The Clerk of the National Assembly
Office of the Clerk
Main Parliament Buildings
Nairobi, Kenya

Attention: S. Njoroge

Re: Submission on The Virtual Asset Service Providers Bill, 2025

We refer to the above subject matter and your public notice dated 11th April 2025, inviting the public to submit their comments on the Virtual Asset Service Providers Bill 2025.

Please see annexed to this letter a schedule, setting out our comments and proposals relating to the Bill. Should you require any clarifications, please do not hesitate to contact us at admin@credence.africa or at +254 719 468240.

Yours Faithfully,

Muthoni Njoroge
For and on behalf of Credence Africa

CREDENCE AFRICA

VIRTUAL ASSET SERVICE PROVIDER COMMENTS FOR SUBMISSION TO THE PARLIAMENTARY COMMITTEE

PART 1

CLAUSE	PROVISION	PROPOSAL	RATIONAL/JUSTIFICATION
2	competent authority” means a relevant regulatory authority or any other body designated as such by the Cabinet Secretary by notice in the Gazette	<p>Amend the definition of “competent authority” to read as follows:</p> <p>“Competent authority” means the Central Bank of Kenya, the Capital Markets Authority, the Competition Authority of Kenya, the Office of the Data Protection Commissioner, the Communications Authority of Kenya, or any other body designated as such by the Cabinet Secretary by notice in the Gazette.”</p>	<p>The current definition of “competent authority” is overly narrow and limited to financial oversight bodies. However, the nature of virtual asset markets demands a cross-sectoral regulatory perimeter. Issues of market conduct, data protection, and digital communications infrastructure intersect directly with how Virtual Asset Service Providers (VASPs) operate in Kenya. Recognizing additional regulators within the statutory definition enhances legal clarity, closes enforcement gaps, and strengthens inter-agency coordination.</p> <p style="text-align: center;">1. Competition Authority of Kenya (CAK)</p> <p>VASPs increasingly operate as digital platforms, marketplaces, and product ecosystems—especially in the case of utility tokens and token-gated access models. This raises key concerns under consumer protection and competition law, including:</p> <ul style="list-style-type: none"> • Misleading or exaggerated claims about token value or use • Referral-based growth models that border on pyramid schemes • Market distortions caused by abuse of dominance in token ecosystems <p>The CAK holds statutory responsibility under the Competition Act and the Consumer Protection Act to address such conduct. It also plays a critical role in supervising business practices that affect pricing, access, and consumer choice. As tokens evolve into</p>

			<p>mainstream consumer-facing products, the CAK must be included as a competent authority to ensure non-financial market harms especially those impacting retail users are properly addressed within the VASP framework.</p> <p>2. Office of the Data Protection Commissioner (ODPC)</p> <p>VASPs collect and process extensive volumes of personal and sensitive data including biometric identifiers, transactional metadata, and behavioral profiles during onboarding, wallet creation, transaction execution, and AML/KYC compliance. In many cases, third-party tools embedded in crypto platforms track users’ activities through blockchain analytics or off-chain behavioral surveillance.</p> <p>ODPC oversight is essential to uphold the rights guaranteed under the Data Protection Act, 2019, particularly regarding:</p> <ul style="list-style-type: none">• Lawful basis for data processing during user onboarding• Consent mechanisms, data minimization, and transparency obligations• Regulation of algorithmic profiling and risk-scoring tools• Compliance with data localization and cross-border transfer rules <p>Virtual assets are increasingly linked to personal identity and digital profiling. Without the explicit inclusion of ODPC, users are left vulnerable to data exploitation and regulators lack clarity on jurisdictional authority. Moreover, aligning with global data protection standards (such as the EU</p>
--	--	--	--

			<p>GDPR) enhances Kenya’s credibility and interoperability in digital markets.</p> <p>3. Communications Authority</p> <p>VASPs rely heavily on communications infrastructure to onboard users, send alerts, advertise products, and conduct customer engagement. Key areas where CAKOM's mandate applies include:</p> <ul style="list-style-type: none"> • Use of telecommunications networks for SMS alerts, USSD codes, and two-factor authentication • Crypto promotions sent via mobile marketing or in-app messaging • Internet-based platforms and content used to advertise, onboard, and interact with users <p>As crypto adoption grows via mobile-based apps, telco-linked wallets, and multi-channel digital outreach, the Communications Authority becomes vital in ensuring compliance with the Kenya Information and Communications Act, including rules on:</p> <ul style="list-style-type: none"> • Consumer protection in digital financial advertising • Oversight of telco partnerships or co-branded wallet services • Mitigation of risks associated with misinformation, fraud, and phishing via digital communications <p>VASPs are not just financial services; they are technology-enabled products deployed through Kenya’s digital infrastructure. Including CAKOM as a competent authority ensures the regulatory framework encompasses the full delivery pipeline of VASP</p>
--	--	--	---

			<p>services especially critical in a market where mobile access is the primary gateway for digital finance.</p> <p>4. Strengthening Institutional Clarity and Legal Certainty</p> <p>Leaving these key regulators to be added later via Gazette notice introduces legal ambiguity and weakens Kenya’s ability to act decisively and in a coordinated fashion across agencies. Clearly listing them in the principal legislation from the outset:</p> <ul style="list-style-type: none"> • Avoids regulatory turf wars or delays in enforcement • Sends a clear signal to industry stakeholders about compliance expectations • Supports whole-of-government regulation of a complex and rapidly evolving market <p>This amendment ensures the Bill reflects the real-world intersection of finance, consumer rights, data governance, and digital infrastructure. This positions Kenya’s VASP regulatory regime as not only credible, but also resilient, adaptive, and fully aligned with the demands of a digital-first economy.</p>
2	<p>“e-money” has the meaning assigned to it under regulation 2 of the National Payment Systems Regulations, 2014;</p> <p>“stablecoin” means a virtual asset designed to or that aims to have its value fixed or pegged relative to one or more reserve assets,</p>	<p>PROPOSAL</p> <p>1. Delete the current definition of “e-money” Remove the existing reference to "e-money" as defined under the National Payment Systems Regulations, 2014. This definition is outdated, unused elsewhere in the Bill, and conceptually incompatible with the</p>	<p>RATIONALE / JUSTIFICATION</p> <p>1. The Current “e-money” Definition Is Outdated and Misaligned with Crypto Architecture The existing definition of “e-money,” adapted from traditional mobile money or prepaid card systems, assumes a centralized issuer, redemption in fiat, and electronic or magnetic storage. These assumptions do not apply to crypto-assets, which often operate without an</p>

	<p>including <i>fiat</i> currency, commodities, or other virtual assets, for the primary purpose of maintaining a stable value of the stablecoin;</p>	<p>operational and technological realities of modern crypto-assets.</p> <p>2. Introduce a new definition for “e-money token” Insert the following definition into Clause 2:</p> <p style="padding-left: 40px;">“e-money token” means a type of crypto-asset that purports to maintain a stable value by referencing the value of one official currency and is intended primarily as a means of payment.</p> <p>3. Replace the definition of “stablecoin” with “asset-referenced token” Reframe the terminology and adopt a broader, functionally inclusive definition that accommodates both fiat-pegged and multi-asset pegged digital assets. Insert the following definition into Clause 2:</p> <p style="padding-left: 40px;">“Asset-referenced token” means a crypto-asset that aims to maintain a stable value by referencing one or more assets, including fiat currencies, commodities, or other crypto-assets, and that may use reserves, algorithms, or other mechanisms to maintain that value.</p>	<p>issuer, are held via distributed ledger systems, and are not redeemable in conventional legal tender. As such, the definition is structurally incompatible with the decentralized and programmable nature of digital assets.</p> <p>2. It Is Unused in the Bill and Creates Potential for Regulatory Misinterpretation The term “e-money” appears nowhere else in the Bill. Its presence serves no operative function and risks creating confusion among regulators or drafters—particularly as digital payment and asset technologies increasingly converge. Removing it prevents misapplication in future subsidiary legislation and avoids conflict with existing financial sector laws, including those governing mobile money.</p> <p>3. Legacy Terminology Obscures Blockchain-Based Storage Models Language such as “electronically or magnetically stored” presumes outdated architecture rooted in banking databases or mobile wallets. Crypto-assets are stored and transferred on blockchain systems, which rely on public-private key infrastructure and consensus mechanisms. The current language fails to capture how blockchain works, thereby introducing legal uncertainty as to whether crypto holdings qualify as “stored value.”</p> <p>4. Redemption Model Embedded in Traditional e-money Does Not Apply to Crypto Under the traditional e-money model, users deposit fiat and receive e-money in return, creating a legal claim on the issuer. Most crypto-assets, including widely used stablecoins, are not redeemable in this way. Some use algorithmic mechanisms, while others are collateralized by offshore assets.</p>
--	---	--	---

			<p>These models do not fit into the one-to-one redemption framework assumed in the current definition and thus fall outside its scope—despite being economically significant and widely used.</p> <p>5. Narrow Scope Fails to Capture Emerging Asset-Referenced and Hybrid Tokens The definition is too limited to account for tokens that reference non-fiat assets such as gold, carbon credits, real estate, or even baskets of digital currencies. These asset-referenced tokens are increasingly used in cross-border payments, remittances, and investment. Regulating them under the same outdated e-money definition would either exclude them or incorrectly classify them, weakening regulatory oversight and limiting the ability to apply fit-for-purpose safeguards.</p> <p>6. Programmability of Digital Assets Is Not Reflected Today’s crypto-assets are programmable instruments capable of automating payments, controlling access, enforcing contracts, or managing investment rights. They are not passive stored value but active financial tools embedded in smart contracts or decentralized applications. A definition that does not reflect programmability risks applying static regulation to dynamic instruments, creating compliance gaps and stifling innovation.</p> <p>7. Replacing “Stablecoin” with “Asset-Referenced Token” Ensures Functional and Legal Precision The term “stablecoin” is too generic and colloquial. Not all such assets are “coins,” and the term does not distinguish between fiat-pegged, commodity-backed, or algorithmic models. A more appropriate term is “asset-referenced token,” which covers any crypto-</p>
--	--	--	--

			<p>asset that seeks value stability by referencing other assets—be it fiat currency, gold, or crypto. This term allows for differentiated regulation and supports risk-based supervision of distinct product types.</p> <p>8. “E-money Token” Accurately Captures Fiat-Pegged Crypto for Payments “E-money token” should be introduced to refer specifically to crypto-assets designed to mirror the value of one official fiat currency and used primarily for payment purposes. This definition provides clarity for applying rules around licensing, redemption, AML/CFT compliance, and capital requirements to a clearly defined class of payment instruments in the crypto ecosystem.</p> <p>9. Strengthens Legal Clarity, Supervisory Tools, and Consumer Protection By introducing clear and forward-looking definitions like “e-money token” and “asset-referenced token,” regulators can tailor rules based on function rather than outdated legal forms. This supports Kenya’s ability to oversee next-generation financial technologies, address systemic risks, and protect consumers engaging with digital assets across payment, savings, and investment use cases.</p> <p>10. Future-Proofs the Legal Framework for Innovation and Global Alignment Removing the legacy “e-money” definition and introducing these crypto-native terms ensures the Bill reflects how the digital asset market actually works. It enables Kenya to establish a legal framework that is forward-compatible with emerging token structures, interoperable with global standards, and</p>
--	--	--	---

			adaptable to new innovations without requiring constant legislative overhaul.						
2	<p>Custodial wallet provider” as: “a person providing custodial wallet services under this Act”;</p> <p>“Custodial wallet” as: “a wallet in which the private keys to the subject’s virtual assets are held and managed by a third party for proof of ownership and facilitation of transactions.”</p>	<p>1. Revised Definitions for Clause 2 (Interpretation)</p> <p>“Custodial wallet provider” Means any natural or legal person that provides safekeeping, administration, or control services in relation to virtual assets on behalf of third parties. This includes private key custody, delegated transaction authority, multi-signature access, escrow-based conditional control, or smart contract-based access management.</p> <p>“Custodial wallet” Means any digital wallet, platform, or contract-based arrangement where virtual assets are stored or made accessible under the control of a third party, whether through key custody, conditional locks, delegated execution rights, or governance protocols.</p> <p>2. Proposed Additions to the First Schedule (Virtual Asset Services)</p> <table><tr><th>Type</th><th>Function</th><th>Description</th></tr><tr><td>Custodial Wallet Services</td><td>Key custody</td><td>Holding and securing private keys on behalf of users for the purpose of enabling safekeeping, access, or recovery of virtual assets.</td></tr></table>	Type	Function	Description	Custodial Wallet Services	Key custody	Holding and securing private keys on behalf of users for the purpose of enabling safekeeping, access, or recovery of virtual assets.	<p>RATIONALE AND JUSTIFICATION</p> <p>1. Revising the Definition of “Custodial Wallet Provider” and “Custodial Wallet” (Clause 2 – Interpretation)</p> <p>1.1 The current definitions rely on a narrow understanding of custody that is based exclusively on the possession and management of private keys. This model originates from traditional finance where physical possession or key control equates to asset control. However, it does not sufficiently address the realities of how virtual assets function in modern financial ecosystems.</p> <p>1.2 In digital environments, control over virtual assets is often exercised through functional authority rather than direct key possession. Service providers may execute transactions through smart contracts, governance roles within decentralized protocols, or platform-level permissions that allow them to enable, block, or redirect user assets. These arrangements introduce custodial risk, even when the service provider does not physically control the key.</p> <p>1.3 The definition must be expanded to reflect a broader and more accurate understanding of custody, one that is based on functional control, delegated authority, and the capacity to influence asset transfer or access. This ensures that the law captures the full range of actors who present risk to users and markets, improves regulatory reach, and strengthens consumer protection.</p>
Type	Function	Description							
Custodial Wallet Services	Key custody	Holding and securing private keys on behalf of users for the purpose of enabling safekeeping, access, or recovery of virtual assets.							

		<p>Escrow Services Conditional custody</p> <p>Administrative Control Transaction execution</p> <p>Delegated Access Platforms Smart contract control</p>	<p>Temporarily holding or restricting transfer of virtual assets based on predetermined conditions, contractual terms, or smart contract triggers.</p> <p>Authorizing, managing, or initiating transactions on behalf of users, including delegated signing authority without holding private keys directly.</p> <p>Operating platforms or protocols that control user asset access through governance rights, multi-signature schemes, time-locks, or protocol-level key control.</p>	<p>2. Disaggregating Virtual Asset Services in the First Schedule</p> <p>2.1 The current structure of the Bill combines multiple functions under the general category of custodial services, without distinguishing between key safekeeping, escrow management, delegated transaction execution, or smart contract-based access control. This aggregation fails to reflect material differences in service delivery, user interaction, and regulatory exposure.</p> <p>2.2 These services vary not only in how they operate technically but also in how they allocate responsibility, define legal relationships, and manage risk. An escrow provider does not have the same obligations as a wallet custodian, and a platform administrator who governs smart contracts performs a function distinct from a delegated transaction signer. Each role creates different legal, operational, and financial risks.</p> <p>2.3 By disaggregating these services into four clearly defined categories—Custodial Wallet Services, Escrow Services, Administrative Control, and Delegated Access Platforms—the Bill can assign more appropriate licensing obligations, tailor compliance expectations, and align regulatory supervision with actual risk. This also promotes legal certainty, supports innovation, and prevents regulatory overreach or underreach.</p> <p>3. Aligning with FATF’s Functional Approach to Regulating Virtual Asset Service Providers</p> <p>3.1 FATF Recommendation 15 requires jurisdictions to regulate entities that perform safekeeping, administration, or control over virtual assets or the</p>
--	--	---	--	---

			<p>tools that enable access to them. This includes actors who do not hold private keys but still facilitate asset transfer, impose transactional restrictions, or execute programmatic logic that impacts users' financial exposure.</p> <p>3.2 Excluding actors such as escrow agents, delegated signers, or smart contract administrators creates regulatory gaps. These roles are critical in decentralized finance, token issuance, and digital marketplaces, where conditional logic and contract automation are central to how assets are handled. If these actors are not brought within the regulatory perimeter, they remain beyond the reach of compliance, enforcement, or investor protection.</p> <p>3.3 Kenya's framework should adopt a risk-based, function-driven definition of regulated activity. This would include any entity that can influence the safekeeping, access, or movement of virtual assets, even when it lacks direct key control. Doing so not only aligns with global regulatory expectations but also prepares the country to supervise emerging technologies that are already reshaping how virtual assets are issued, held, and transacted.</p>
			<p>4. Assigning Regulatory Oversight Based on Functional Risk Exposure</p> <p>4.1 Each service function introduces a specific type of regulatory risk and should therefore fall under the authority of the regulator best positioned to supervise it. Attempting to place all supervisory duties under a single authority would create blind spots and dilute enforcement capability.</p>

			<p>4.2 Custodial wallet services, where client assets are stored or safeguarded, raise prudential and operational risks. These are aligned with the mandate of the Central Bank of Kenya, which already oversees financial institutions with similar responsibilities.</p> <p>4.3 Escrow services may relate to payment systems or capital market instruments. Where escrow is used for token issuance or investor settlements, the Capital Markets Authority should be the lead regulator. Where escrow supports transaction settlement or remittances, the Central Bank has jurisdiction.</p> <p>4.4 Administrative control functions, where a service provider initiates or approves transactions on behalf of users, carry market conduct and investor risk. These should be supervised by the Capital Markets Authority. Where such control involves data profiling, algorithmic decision-making, or access delegation based on personal identifiers, the Office of the Data Protection Commissioner must also be involved.</p> <p>4.5 Delegated access platforms, such as those that run decentralized applications or manage protocol-level smart contracts, introduce systemic infrastructure risk. These platforms should be subject to joint oversight by the Capital Markets Authority, the Office of the Data Protection Commissioner, and the Communications Authority of Kenya, which is best placed to regulate digital infrastructure and telecom-based wallets.</p> <p>4.6 No single regulator currently has the full mandate, tools, or expertise to oversee all four categories. A shared supervisory model is therefore required to ensure comprehensive oversight, avoid jurisdictional</p>
--	--	--	--

			<p>fragmentation, and enable proactive enforcement across the virtual asset sector.</p> <p>5. Establishing an Umbrella Definition Supported by Specific Service Classifications</p> <p>5.1 The Bill should incorporate a general definition of custodial services as any activity involving the safekeeping, control, conditional holding, or delegated access to virtual assets on behalf of another party. This creates a high-level legal anchor for oversight and licensing.</p> <p>5.2 Within the First Schedule, the law should enumerate specific regulated functions under this umbrella that is custodial wallets, escrow services, administrative control, and delegated access platforms. This two-tier structure provides clarity for both legal interpretation and regulatory implementation.</p> <p>5.3 It also future-proofs the legal framework. By organizing around functional activity rather than legacy institutional models, the law can respond quickly to innovations in tokenization, automated financial contracts, and multi-party governance systems without needing constant amendment.</p> <p>6. Strategic Opportunity to Position Kenya as a Modern Digital Asset Regulator</p> <p>6.1 A legal framework that combines multiple service categories under a generic definition risks creating enforcement uncertainty, regulatory inefficiency, and weak investor safeguards. It also leaves room for high-risk operators to avoid accountability by exploiting definitional loopholes.</p>
--	--	--	---

			<p>6.2 By adopting a function-based, risk-informed, and regulator-aligned classification of virtual asset services, Kenya can set a new standard in digital asset oversight across the continent. This will position the country as a reliable jurisdiction for responsible innovation and provide a foundation for cross-border digital finance partnerships.</p> <p>6.3 Such a framework will also increase market confidence by ensuring that all service providers—regardless of their technical architecture—are subject to appropriate rules, clear duties, and effective regulatory oversight. This is essential for building a credible and inclusive digital finance ecosystem that serves the public interest.</p>
2	<p>“Issuer” means a person who is authorised to issue a virtual asset offering under this Act.</p> <p>“Virtual asset offering” means a method of raising funds whereby an issuer issues virtual assets and offers them in exchange for funds.</p>	<p>Delete and replace with:</p> <p>“Issuer” means a natural or legal person, or any other undertaking, that creates, originates, or otherwise makes available crypto-assets to the public, either through an initial offering or any subsequent issuance mechanism.”</p> <p>Delete and replace with:</p> <p>“Initial virtual financial asset offering” means a method of raising funds whereby an issuer is issuing virtual financial assets and is offering them in exchange for fiat currency or other virtual assets.”</p> <p>Introduce complementary definitions:</p>	<p>RATIONALE / JUSTIFICATION</p> <p>The current definitions of “issuer” and “virtual asset offering” are overly narrow, structurally outdated, and insufficient to address the operational realities of today’s crypto-asset ecosystem. They focus exclusively on initial, formally authorized offerings, without accounting for the diverse, decentralized, and ongoing nature of token issuance in global and local markets. This undermines legal enforcement, regulatory oversight, and consumer protection in Kenya. The following issues illustrate why reform is essential:</p> <ol style="list-style-type: none"> 1. Definition Limits Enforcement to Authorized Issuers Only By defining an issuer solely as someone authorized under this Act, the Bill inadvertently excludes unlicensed or rogue issuers who are often the highest-risk actors in token markets. These may include promoters

		<p>‘applicant issuer’ means an issuer of asset-referenced tokens or e-money tokens who applies for authorisation to offer to the public or seeks the admission to trading of those crypto-assets;</p> <p>‘offer to the public’ means a communication to persons in any form, and by any means, presenting sufficient information on the terms of the offer and the crypto-assets to be offered so as to enable prospective holders to decide whether to purchase those crypto-assets;</p>	<p>of scams, fraudulent projects, or foreign entities targeting Kenyan citizens online. Without including all persons or undertakings who engage in token issuance, enforcement is severely weakened, and investor protection is compromised.</p> <p>2. Fails to Capture Decentralized and Programmatic Issuance Structures A growing share of crypto-assets are issued through decentralized autonomous organizations (DAOs), protocol-level governance votes, or automatically via smart contracts. These issuance models lack a traditional legal “issuer” but still pose financial, governance, and consumer risks. The definition must be broadened to cover these undertakings, ensuring that the law captures all issuance activity regardless of organizational form or degree of centralization.</p> <p>3. Overemphasis on Initial Offerings Ignores Ongoing and Secondary Issuance The current framing treats issuance as a one-time, IPO-like event. In reality, token supply is often dynamic expanded through staking rewards, liquidity incentives, protocol forks, or inflationary mechanisms. These subsequent issuance events significantly impact market prices, token utility, and consumer exposure. Excluding them from regulation creates loopholes and distorts the market’s regulatory perimeter.</p> <p>4. No Jurisdictional Reach Over Cross-Border Issuers Targeting Kenya Many crypto offerings originate from outside Kenya but directly target Kenyan users through websites, social media, and digital platforms. A definition that requires domestic authorization excludes these actors from</p>
--	--	---	--

			<p>oversight. By redefining issuance as the act of making crypto-assets available to the public, the Bill can extend legal jurisdiction to all token offers made to Kenyan residents, regardless of where the issuer is based.</p> <p>5. Unclear Meaning of “Funds” Reduces Coverage of Common Offering Structures The phrase “in exchange for funds” is ambiguous. It is unclear whether this includes only fiat currency or also crypto-assets such as ETH or USDT, which are now the dominant forms of consideration in token sales. If interpreted narrowly, offerings settled in crypto could fall outside the Bill’s scope. Clarifying this point ensures that materially similar transactions are treated with equal regulatory scrutiny.</p> <p>6. Staking Rewards Resemble Gaming Incentives and Pose AML/CFT Risks Staking rewards distribute tokens based on participation, often using algorithmic rules or probabilistic returns. This resembles betting or gaming, where users stake value and receive variable returns. Kenya already regulates the gaming sector and has brought it under the AML reporting regime due to its susceptibility to abuse. Excluding staking-based issuance from this Bill opens a regulatory gap where virtual assets operate with gaming-like risk and reward profiles without consumer protection or AML safeguards. Including these models in the scope of “offerings” ensures regulatory consistency across digital financial services and protects the integrity of Kenya’s AML/CFT framework.</p> <p>7. Exclusion of Airdrops, Rewards, and Indirect Offerings Enables Regulatory Arbitrage Token distributions today occur through</p>
--	--	--	--

			<p>airdrops, loyalty schemes, bundled purchases, and non-cash compensation models. While not direct “sales,” they often result in tradable crypto-assets with market value. Bad actors can exploit the current narrow definition to avoid compliance by disguising offerings through these structures. A functional, effect-based definition ensures that issuance is regulated based on the risks and outcomes it creates not its form.</p> <p>8. Ambiguity Around Accountability of Unlicensed Issuers When the law recognizes only authorized parties as “issuers,” it becomes unclear who bears responsibility for tokens created outside the licensing regime. This ambiguity weakens enforcement in cases of fraud, misinformation, or operational failure. By defining issuer status based on conduct (i.e., creation or distribution of tokens to the public), the law can hold all actors accountable, regardless of registration status.</p> <p>9. Lack of Supporting Definitions Weakens Supervision and Disclosure Rules The absence of terms like “applicant issuer” and “offer to the public” limits the legal framework’s ability to enforce licensing, disclosures, whitepaper standards, and advertising rules. These complementary definitions are essential for creating a structured and predictable regulatory environment that treats investor communication and offering mechanics with appropriate oversight.</p> <p>10. Misalignment with Global Standards Limits Kenya’s Regulatory Credibility Globally, regulators have adopted more flexible definitions that focus on the activity and impact of token issuance—not just on the</p>
--	--	--	---

			<p>legal status of the issuer. These definitions recognize that issuance can be centralized, decentralized, one-time, or continuous. Kenya’s current language falls behind these trends. Adopting broader, function-based definitions ensures Kenya keeps pace with international norms, facilitates cross-border regulatory cooperation, and positions the country as a credible destination for compliant innovation.</p>
2	<p>“virtual asset” means a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes and does not include digital representation of fiat currencies, e-money, securities and other financial assets;</p>	<p>Delete the current definition of “virtual asset” and replace it with the following internationally aligned and technology-neutral definition:</p> <p>“Virtual asset” means a digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily attached to a legally established currency, and is capable of being transferred, stored, or traded electronically. It may be used for payment, investment, or access to goods, services, or rights. It excludes digital representations of fiat currency, e-money, securities, or other financial instruments regulated under separate legislation.”</p>	<p>The definition of “virtual asset” is the legal cornerstone of the entire Virtual Asset Service Providers (VASP) framework. It determines what falls within regulatory scope and what does not. A narrow or vague definition risks either overregulating low-risk use cases or underregulating high-risk ones. The current Kenyan definition is too limited in scope and fails to reflect the diversity, structure, and real-world use of crypto-assets. It should be replaced with a broader, more precise formulation that is legally coherent and globally consistent.</p> <p>1. The current definition relies on subjective economic functions</p> <p>By tying regulatory scope to whether a token “can be used for payment or investment,” the definition introduces unnecessary vagueness. Many tokens today serve multiple or evolving functions. A token may be designed for utility (such as platform access or governance) but gain investment-like characteristics over time through trading or staking. Others may be held for community participation or access rights, yet still represent value.</p>

			<p>A regulatory perimeter based only on economic use introduces interpretational uncertainty and weakens legal enforceability. The proposed definition avoids subjective use tests and instead focuses on inherent functional attributes whether a digital representation of value is transferable, tradable, or storable electronically. This removes ambiguity and improves regulatory clarity.</p> <p>2. It fails to capture modern crypto instruments beyond payment and investment tokens</p> <p>Crypto-asset ecosystems now encompass a wide range of token types, including:</p> <ul style="list-style-type: none"> • Utility tokens used to access services or digital products; • Governance tokens that confer voting rights in decentralized autonomous organizations (DAOs); • NFTs that represent intellectual property, royalties, or fractional rights; • Programmable tokens with embedded logic or automated distribution mechanisms. <p>These assets may not neatly fall into “payment” or “investment” categories but still carry economic significance and user risk. The updated definition broadens the scope to cover access rights, governance, and digital services, which are increasingly central to blockchain economies.</p> <p>3. The exclusion clause lacks legal clarity and coordination with existing laws</p> <p>The phrase “does not include digital representation of fiat currencies, e-money, securities and other financial</p>
--	--	--	---

			<p>assets” is insufficiently precise. It fails to define or cross-reference what constitutes a “security” or “financial asset” under Kenyan law, potentially creating overlap or conflict with the Capital Markets Act, the Central Bank of Kenya Act, and the National Payment Systems Act.</p> <p>The revised definition remedies this by stating that excluded instruments are those regulated under separate legislation, thereby respecting Kenya’s regulatory architecture while maintaining legal clarity. It allows for harmonisation between regulators and prevents jurisdictional conflicts between CBK, and CMA.</p> <p>4. It does not reflect decentralization, programmability, or smart contract functionality</p> <p>Modern crypto-assets are not only digital values but automated financial instruments, managed through smart contracts, DAOs, and programmable logic. These characteristics introduce governance complexity, execution risk, and cyber exposure. A static definition based solely on tradeability or economic intent ignores the technological dimension of risk and operation.</p> <p>The FATF framework recognize the need for technology-neutral language. By emphasizing whether the asset is stored, transferred, or traded electronically, the proposed definition incorporates the underlying technological traits of blockchain systems without over-relying on economic intent.</p> <p>5. Global regulatory coherence requires convergence with FATF standards</p>
--	--	--	---

			<p>Kenya’s ambition to become a credible jurisdiction for digital innovation requires alignment with international financial integrity and market development standards. The FATF defines virtual assets based on functionality and risk, not by economic purpose alone. Setting a broad perimeter and using sub-classifications (e.g., e-money tokens, asset-referenced tokens, utility tokens) ensures appropriate, proportionate regulation.</p> <p>Adopting this updated definition would ensure:</p> <ul style="list-style-type: none"> • Ensure compatibility with AML/CFT frameworks under FATF; • Improve cooperation with international regulators, central banks, and financial intelligence units; • Provide market certainty for innovators, exchanges, wallet providers, and token developers; • Future-proof its legal framework against new and hybrid token models. <p>6. A modern definition enables more robust consumer protection and systemic oversight</p> <p>Digital assets that do not fall under clearly defined regulatory categories can pose systemic risks especially when their legal treatment is unclear. A broader and precise definition ensures that any product marketed to the public as a store of value, medium of exchange, or access token is within scope, regardless of the label it carries.</p> <p>This allows regulators to apply disclosure rules, conduct supervision, licensing requirements, and enforcement powers consistently. It also reduces the</p>
--	--	--	--

			risk of regulatory arbitrage, where actors design token structures to deliberately avoid compliance.
2	virtual service token” means a digital representation of value which is not transferable or exchangeable with a third party at any time and includes digital tokens whose sole function is to provide access to and application of service or to provide a service or function directly to its owner; and	<p>Proposal</p> <p>“Virtual service token” means a type of crypto-asset that is intended solely to grant digital access to a specified good, content, service, or function provided within a closed or limited ecosystem and does not confer any rights of ownership, profit participation, payment, redemption, investment return, or governance in respect of the issuer or any third party.</p> <p>A token shall not be deemed a virtual service token if it:</p> <p>(a) is transferable or exchangeable, directly or indirectly, for fiat currency or any other crypto-asset;</p> <p>(b) is used or marketed as a means of payment, investment, or value transfer outside the limited ecosystem in which access is granted;</p> <p>(c) is traded, or reasonably expected to be traded, on a crypto-asset exchange, decentralized protocol, or peer-to-peer marketplace; or</p> <p>(d) is offered, advertised, or promoted in a manner that implies speculative value, resale potential, or capital gain</p> <p>e) is a utility token or a non-financial access token</p>	<p>RATIONALE / JUSTIFICATION</p> <ol style="list-style-type: none"> 1. Ensures Regulatory Precision Based on Economic Function, Not Label The current definition hinges on the issuer’s stated purpose rather than how the token behaves in practice. This opens the door to regulatory evasion. The revised wording adopts a function-based approach that considers how the token is used, whether it is transferable, marketed for gain, or traded—regardless of its original intent or technical design. This aligns with evolving international norms that classify tokens by their actual economic impact, not superficial features or promotional claims. 2. Prevents Misuse of the Utility Token Label to Avoid Oversight Many token issuers design products that confer access to services while embedding economic rights such as tradability or speculative resale. These tokens are often promoted as “utility tokens” to escape financial regulation. The amended definition makes it clear that once a token is designed, promoted, or expected to function as a payment or investment tool, it ceases to qualify as a pure service token and must be regulated accordingly. This distinction is vital to protect consumers from disguised investment schemes. 3. Addresses the Reality of Programmable Tokens and Evolving Features Tokens today can evolve after issuance through smart contract upgrades, bridging, wrapping, or governance proposals that alter their use. A token that begins as an access tool

		<p>“Utility token” means a crypto-asset that is intended to provide access to a specific digital application, network, platform, or protocol, and that may be used within such platform to consume services, interact with features, or activate functions, but which does not entitle the holder to any financial return, asset backing, or governance right beyond its defined utility function.</p> <p>“Non-financial access token” means a digitally issued token that confers access to a personal, non-transferable service, such as memberships, subscriptions, event access, or digital entitlements, and is neither tradable nor exchangeable outside the issuer’s-controlled environment.</p>	<p>may later gain exchangeability or profit-sharing functions. The updated definition focuses on actual market behavior, making it possible to reclassify and regulate tokens as they change in function, rather than relying on static definitions.</p> <p>4. Protects Genuine Access-Based Innovation There is a legitimate category of tokens that serve purely as keys to content, platforms, or services and are not tradable or used as stores of value. The revised definition maintains a safe legal space for such tokens, shielding them from unnecessary regulatory burden while drawing clear limits: once a token is used as money, invested in, or traded on exchanges, it must be treated as a virtual asset.</p> <p>5. Improves Legal Clarity and Enforceability Phrases such as “not transferable or exchangeable... at any time” are legally ambiguous and difficult to enforce. The revised clause offers specific, testable conditions such as whether a token is actually traded, can be exchanged for fiat or other crypto-assets, or is promoted with profit expectations. This makes the framework actionable for regulators and interpretable by courts.</p> <p>6. Captures Risks from Emerging Use Cases Including DeFi and GameFi Tokens in digital games, decentralized applications, or content platforms increasingly resemble financial instruments. Some are exchangeable, carry market value, and are distributed in reward-based or gamified structures that mimic gambling or investment behavior. The revised definition ensures that tokens functioning like money or securities, even if embedded in entertainment platforms, are subject to proper supervision.</p>
--	--	---	---

			<p>7. Mitigates Regulatory Arbitrage and Enhances Supervisory Consistency Without a function-based definition, token issuers can easily restructure offerings to exploit gaps between service token exemptions and investment-related obligations. This leads to inconsistent supervision, undermines consumer confidence, and weakens the credibility of the regulatory framework. The proposed definition closes these loopholes by setting clear boundaries for what qualifies as a service token and what does not.</p>
			<p>This refined rationale supports the adoption of a definition that is practical, enforceable, and future-ready- a future that protects innovation while ensuring that economically active tokens are brought under appropriate oversight. Let me know if you would like the accompanying legislative text or if you would like this packaged into a formal legal brief or policy note.</p>
2	<p>“Virtual asset trading platform” means a digital platform— (a) which facilitates the exchange and trading of virtual assets for fiat currency or other virtual assets on behalf of third parties for a fee, commission or other benefit; and (b) which— (i) holds custody or controls virtual assets on behalf of its clients to facilitate an</p>	<p>PROPOSED AMENDMENT</p> <p>“Virtual asset trading platform” means any digital interface, software protocol, or technological infrastructure whether centralized, decentralized, or hybrid that facilitates the exchange, trading, or matching of virtual assets with other virtual assets or fiat currency, on behalf of users or participants, and which derives direct or indirect economic benefit from such facilitation.</p>	<p>RATIONALE / JUSTIFICATION</p> <p>1. Captures Both Centralized and Decentralized Models The current definition assumes custodial control or principal-agent intermediation. This excludes non-custodial platforms and automated trading systems such as decentralized exchanges (DEXs), automated market makers (AMMs), and smart contract-based marketplaces. These platforms execute high-value transactions without holding user assets, yet introduce similar market, consumer, and AML/CFT risks.</p>

	<p>exchange; or (ii) purchases virtual assets from a seller when transactions or bids and offers are matched in order to sell them to a buyer.</p>	<p>This includes, but is not limited to:</p> <ul style="list-style-type: none"> (a) platforms that match, aggregate, or execute trades between counterparties; (b) systems that provide or integrate access to liquidity pools, automated market makers, or smart contracts for trading purposes; (c) entities that exercise custodial or administrative control over virtual assets to facilitate exchange, settlement, or order execution; (d) operators that act as principal to the trade by purchasing virtual assets from a seller for onward sale to a buyer; and (e) service providers offering decentralized interfaces, protocols, or algorithms that perform these functions autonomously or via delegated access. <p>A platform shall be deemed a virtual asset trading platform if it enables users in Kenya to transact, irrespective of its place of incorporation, operational model, or underlying technology.</p>	<p>2. Aligns Regulation with Function, Not Structure Modern trading platforms are no longer confined to traditional exchange models. Peer-to-peer protocols, interface-only platforms, and algorithmic liquidity protocols now perform core trading functions. The revised definition focuses on functional conduct that is what the platform does, rather than how it is structured or where it is domiciled.</p> <p>3. Encompasses Smart Contract-Based and Protocol-Level Trading Trading platforms today may operate entirely through code without a human intermediary. These platforms still require regulatory scrutiny where they:</p> <ul style="list-style-type: none"> • Route transactions, • Set trading parameters, • Facilitate pricing through oracles or token pairs, or • Enable real-time asset transfer. <p>A legal definition must reflect these realities.</p> <p>4. Includes Platforms Acting as Principals Some platforms purchase crypto-assets in bulk from sellers and re-sell them to buyers (e.g., broker-dealer models). The current law omits these principal-based structures unless custody is involved. This risks leaving some high-risk trading models unlicensed.</p> <p>5. Closes Jurisdictional Loopholes in Cross-Border Access Without an extraterritorial trigger, offshore exchanges can claim to fall outside local regulation even while actively targeting Kenyan users through web portals, apps, influencers, or marketing campaigns. The revised definition establishes jurisdiction based on</p>
--	--	--	--

			<p>user access, not platform location, in line with international AML and investor protection norms.</p> <p>6. Supports Proportional Licensing and Tiered Regulation</p> <p>By clearly identifying platform functions eg matching, custody, execution, or settlement. The new definition enables risk-based licensing regimes. Different types of platforms can be subjected to different regulatory burdens depending on function, risk profile, and user base.</p>
Clause Section 3(1)	A person is a virtual asset service provider if that person is a local company incorporated under the Companies Act or a foreign company with a certificate of compliance under the Act.	<p>Proposal</p> <p>Amend to: "A virtual asset service provider means any natural or legal person, or other undertaking, that conducts one or more of the activities listed in the First Schedule, regardless of legal form or licensing status, and whether centralised or decentralised."</p>	<p>Rationale</p> <p>The current provision wrongly limits the scope to only incorporated and licensed entities, creating a regulatory blind spot. FATF Recommendation 15 applies to both natural and legal persons engaged in VASP functions, even if unlicensed. Decentralised services and peer-to-peer platforms must be captured to prevent regulatory arbitrage and uphold AML/CFT obligations. This proposal ensures function-based rather than form-based coverage.</p>
Section 3(2)	Virtual service tokens are not virtual assets and service providers dealing with them are exempt from licensing.	Delete blanket exemption. Replace with: "Service tokens that are non-transferable, non-tradable, and non-exchangeable may be exempt, provided they meet criteria set by the regulator through subsidiary legislation."	Blanket exclusion invites misclassification and abuse. Under FATF guidance and international practice, any token functioning as a means of payment or investment must fall within the regulatory perimeter. The revised proposal introduces a functional test, ensuring that economic substance, not labels, determines scope. This also reflects emerging practices, which use functionally grounded exemption criteria.
Section 4	The main object is to license and regulate the activities of virtual asset service providers in and from Kenya.	Amend to: "To license and regulate virtual asset activities in and from Kenya, in line with risk-based principles, international standards, and obligations under anti-money laundering and consumer protection frameworks."	The current clause lacks clarity on regulatory purpose and alignment with FATF obligations. The proposed language integrates financial integrity objectives and supports the policy intent behind digital asset regulation, including systemic risk mitigation and consumer protection. The VASP regime must signal regulatory seriousness and readiness to international partners and investors.
Section 5(2)	Excludes digital value within closed ecosystems, fiat currencies issued by central	"This Act shall not apply to instruments or systems explicitly excluded by the regulator on	Overly broad exclusions undermine flexibility and responsiveness. Market dynamics shift, and instruments like NFTs and closed-loop tokens can evolve into financial

	banks, and NFTs not used for financial purposes.	the basis of a published risk assessment and subject to periodic review."	assets. A regulator-led exemption framework ensures adaptive oversight. Functional and risk-based exclusions offer better protection than static legislative carve-outs.
--	--	---	--

PART 2

CLAUSE	CURRENT PROVISION	PROPOSED CHANGES	RATIONALE/JUSTIFICATION
Section 6	Designates the Capital Markets Authority, the Central Bank of Kenya, and any other body designated by the Cabinet Secretary as the regulatory authorities under the Act.	<p>Proposed Amendment: Revise Section 6 to explicitly allocate regulatory mandates based on the nature of the virtual asset service or product, referencing the functional categories outlined in the First Schedule. As currently worded, the clause implies that all listed authorities have jurisdiction over all matters, which creates ambiguity for license applicants and risks regulatory overlap. A clarified structure should read:</p> <ul style="list-style-type: none"> • The CBK shall be responsible for oversight of payment-related virtual assets and services, including e-money tokens, stable payment tokens, and custodial wallet functions involving value storage or transmission. • The CMA shall regulate investment-oriented virtual assets, capital-raising mechanisms (such as token offerings), decentralized finance (DeFi) instruments, and platforms facilitating trading or investment access. • Where applicable, the Office of the Data Protection Commissioner (ODPC) and Communications Authority of Kenya (CA) shall exercise concurrent jurisdiction over 	<p>Rationale / Justification:</p> <ol style="list-style-type: none"> 1. Eliminates Jurisdictional Ambiguity Clarifying which regulator governs which service class prevents institutional conflict, avoids double licensing, and supports coherent regulatory guidance for applicants. 2. Aligns with FATF's Risk-Based and Multi-Agency Oversight Model FATF Recommendation 15 encourages the use of specialized agencies based on risk type—financial integrity, consumer protection, and systemic risk—ensuring that no single body bears impractical or inappropriate oversight burdens. 3. Supports Legal Certainty and Market Confidence Service providers, investors, and compliance professionals require clarity on where to file applications, make disclosures, and obtain guidance. This amendment fosters predictability and reinforces institutional accountability.

		<p>services that process personal data or leverage digital communications infrastructure.</p> <ul style="list-style-type: none"> • The Cabinet Secretary may designate other sectoral regulators to co-supervise niche services through gazetted regulations. Eg SACCOS when that market matures 	
Section 7	Lists the powers and functions of the regulatory authorities.	<p>Proposed Amendment: Revise Section 7 to include clear, risk-sensitive, and accountability-based powers with codified inter-agency coordination and transparency mechanisms. The revised clause should state:</p> <p>7(1) The relevant regulatory authorities shall exercise their functions in accordance with the following principles:</p> <p>(a) Risk-Based Supervision – Regulatory action and licensing requirements shall be proportionate to the nature, scale, complexity, and risk profile of the virtual asset service provider or activity.</p> <p>(b) Functional Allocation – Each regulatory authority shall act within its designated jurisdiction as defined under Section 6 and the First Schedule.</p> <p>(c) Collaborative Regulation – Regulatory authorities shall enter into binding Memoranda of Understanding (MoUs) to ensure consistent supervisory approaches, information sharing, and cross-border cooperation.</p> <p>(d) Public Guidance and Consultation – All binding rules, codes, or circulars with industry impact must be preceded by public</p>	<p>Issues Identified with Current Clause:</p> <ol style="list-style-type: none"> 1. No Reference to Risk-Based Supervision The current provision enables blanket regulation without tailoring oversight to the specific risks posed by different types of virtual asset service providers (VASPs). 2. Absence of Formal Coordination Protocols In an environment involving multiple regulators, failure to mandate MoUs or structured cooperation leads to jurisdictional friction, duplicative compliance burdens, or systemic oversight failures. 3. Vague Guidance Mandate The powers to issue guidelines and notices are overly broad and could result in fragmented or unclear regulatory expectations if not transparently grounded in process. <p>Rationale / Justification:</p> <ol style="list-style-type: none"> 1. Risk-Based Regulation Aligns with Global Best Practice FATF's Recommendation 15, endorse risk-based supervision as a core operating principle for virtual asset regulation. It ensures regulatory resources are focused on the

		<p>notice and a comment period of not less than 21 days unless issued in emergency.</p> <p>(e) Annual Reporting – Each regulatory authority shall submit an annual report to Parliament detailing:</p> <ul style="list-style-type: none"> • Licensing activity and compliance outcomes, • Enforcement actions taken, • Risk assessments conducted, and • Recommendations for regulatory improvement. <p>7(2) The regulatory authorities may issue joint guidance or circulars on matters requiring cross-functional supervision including:</p> <p>(a) Virtual asset custody and safekeeping;</p> <p>(b) Decentralized finance protocols;</p> <p>(c) Cross-border offerings and offshore token issuers targeting Kenyan residents;</p> <p>(d) Data protection and cybersecurity in blockchain systems.</p>	<p>highest-risk activities without stifling innovation.</p> <p>2. Multi-Agency Coordination is Critical for Systemic Oversight Virtual asset ecosystems span financial markets, payments infrastructure, data governance, and consumer protection. Effective regulation must be co-created and co-enforced across specialized authorities to avoid gaps and overlaps.</p> <p>3. Public Transparency Builds Market Trust By requiring prior consultation, publication of enforcement outcomes, and parliamentary reporting, the regulatory framework enhances its legitimacy, improves predictability for market actors, and signals Kenya’s commitment to responsible innovation governance.</p>
Section 8	<p>Outlines that regulatory authorities shall be guided by the principles of:</p> <ul style="list-style-type: none"> • Ensuring financial stability, • Ensuring market integrity (duplicated), • Fostering innovation, fairness, transparency, and efficiency, 	<p>Proposed Legislative Clause:</p> <p>8. In exercising their powers and discharging their functions under this Act, the relevant regulatory authorities shall be guided by the following principles—</p> <p>(a) To safeguard the integrity, stability, and resilience of the financial and virtual asset ecosystem;</p>	<p>Identified Issues with Current Clause:</p> <p>1. No Explicit Reference to Consumer and Investor Protection Modern regulatory frameworks emphasize the protection of retail users and institutional investors, particularly in the face of fraud, rug-pulls, and data exploitation in virtual asset markets.</p> <p>2. Absence of Proportionality and Risk-Based Supervision</p>

	<ul style="list-style-type: none"> Preventing conduct harmful to Kenya's financial reputation. 	<p>(b) To promote a proportionate and risk-based approach to regulation that aligns regulatory requirements with the scale, complexity, and risk profile of the service provider or activity;</p> <p>(c) To ensure the protection of consumers, users, and investors, including safeguards against fraud, unfair practices, financial loss, and systemic exploitation;</p> <p>(d) To foster responsible innovation, fair competition, and open market access while maintaining regulatory certainty for entrepreneurs and developers;</p> <p>(e) To promote financial inclusion through equitable access to virtual asset services, especially for underserved or excluded segments of the population;</p> <p>(f) To enhance transparency, accountability, and procedural fairness in regulatory guidance, licensing, and enforcement processes;</p> <p>(g) To encourage domestic and cross-border cooperation between regulators, competent authorities, and international standard-setting bodies for the effective supervision of virtual asset activities;</p> <p>(h) To prevent the abuse of virtual asset systems for money laundering, terrorism financing, market manipulation, or the circumvention of national laws and public policy objectives.</p>	<p>Without a mandate for proportionality, smaller innovators and lower-risk actors face excessive compliance burdens. This inhibits responsible innovation and creates a compliance-heavy environment without corresponding gains in oversight.</p> <p>3. Omission of Financial Inclusion and Global Cooperation Virtual assets offer unique inclusion opportunities in developing markets. Regulation must actively support their safe adoption. Additionally, oversight of borderless digital systems demands statutory provisions for information exchange and regulatory alignment across borders.</p> <p>4. Drafting Error – Repetition of Subclause (b) The duplicated clause weakens the structural clarity of the Bill and invites interpretation challenges.</p> <p>Rationale / Justification:</p> <p>1. Aligns with Global Standards for Digital Asset Supervision Risk-based and proportionate regulation is a core principle of FATF Recommendation 15 and is embedded in leading digital asset frameworks globally. This approach enables differentiated treatment of low-risk actors while maintaining high-risk guardrails.</p> <p>2. Protects Consumers and Investors in High-Volatility Markets Explicitly including consumer protection empowers regulators to act preemptively</p>
--	---	---	--

			<p>against market abuse and failure, bolstering investor confidence and reputational integrity.</p> <p>3. Supports Financial Innovation and Market Access By emphasizing fairness, transparency, and inclusion, the Act builds a competitive environment that attracts responsible innovation and foreign investment while safeguarding vulnerable populations.</p> <p>4. Strengthens Legal Coherence and Enforceability Codifying these guiding principles as statutory benchmarks ensures all subsequent regulations, circulars, or enforcement actions adhere to a transparent and predictable legal logic.</p>
--	--	--	--

PART III — LICENSING REQUIREMENT

CLAUSE	CURRENT PROVISION	PROPOSAL	RATIONALE
Section 9(1)-(3)	Licensing requirement for any person conducting VASP business in or from Kenya	"9(2) For the avoidance of doubt, a natural person or a startup, or a micro enterprise shall not carry on, or purport to carry on, in or from within Kenya, the business of virtual asset services, unless operating under a regulatory sandbox or simplified licensing regime as prescribed by the relevant regulatory authority."	<p>Issue: Absence of a differentiated regime for low-risk and high-risk virtual asset service providers (VASPs); absolute prohibition on natural persons is overly restrictive.</p> <p>Rationale and Justification:</p> <ol style="list-style-type: none"> 1. FATF Recommendation 15 encourages proportionality in regulation. 2. Provide exemptions or simplified regimes for micro-entities. 3. Supports innovation by enabling small-scale operators to test solutions under controlled conditions.

Section 10		<p>Proposed Amendment:</p> <p>"10(2) The relevant regulatory authority shall issue guidelines that classify virtual asset services by risk tier and provide corresponding supervisory expectations. Such guidelines shall include: (a) a tiered licensing framework based on size, complexity, and risk; (b) thresholds for exempted or simplified licensing for low-risk activities."</p>	<p>Issue: Over-reliance on Schedule without direct statutory clarification of authority roles; absence of risk classification in licensing criteria.</p> <p>Rationale and Justification:</p> <ol style="list-style-type: none"> 1. Creates a framework which tier licenses based on activity class. 2. Enhances predictability and supervisory focus, in line with FATF's risk-based approach.
	Section 11	<p>Proposed Amendment:</p> <p>"11(6) The relevant regulatory authority shall maintain and publish a public register of all licensed virtual asset service providers, including details of the license status, class of license, and principal business address."</p>	<p>Issue: Evaluation criteria in 11(5) and Section 12 overlap; does not require public register of licensees or licensing decisions.</p> <p>Rationale and Justification:</p> <ol style="list-style-type: none"> 1. FATF guidance mandates public registers to improve transparency. 2. Enhances market trust and facilitates AML compliance by counterparties.
	Section 12	<p>Proposed Amendment:</p> <p>"12(h) the likelihood that the service shall promote innovation, environmental sustainability, financial inclusion, and benefits to consumers." "12(m) whether the applicant has been afforded an opportunity to respond to any adverse findings"</p>	<p>Issue: Lacks specificity on ESG and innovation considerations; weak procedural transparency.</p> <p>Rationale and Justification:</p> <ol style="list-style-type: none"> 1. Reflects inclusion of sustainability criteria and weeds out predatory services 2. Ensures adherence to administrative fairness and good regulatory practice.

		prior to final determination of licensing."	
	Section 13	<p>Proposed Amendment:</p> <p>"13(5) A person aggrieved by a licensing condition, rejection, or variation shall have a right to apply for internal review and appeal to the Financial Services Tribunal within thirty days."</p>	<p>Issue: Broad discretion without binding procedural safeguards; no appeal mechanism.</p> <p>Rationale and Justification:</p> <ol style="list-style-type: none"> 1. Reinforces procedural fairness. 2. Explicitly provide appellate frameworks to challenge supervisory decisions.
Section 14–16		<p>Proposed Amendment:</p> <p>"14(2) A license shall be renewable annually subject to ongoing compliance and the payment of the prescribed renewal fee."</p> <p>"16(1)(f) the licensee has repeatedly breached fair market conduct obligations, including misrepresentation or conflicts of interest."</p>	<p>Issue: No automatic renewal framework or conditions for suspension tied to market conduct principles.</p> <p>Rationale and Justification:</p> <ol style="list-style-type: none"> 1. Introduces clarity and business continuity. 2. Provides guidelines on cause-based revocation.
Section 17(1)	A licensee may surrender its license by giving a prior notice for surrender accompanied by a list of documents.	<p>Proposed Amendment:</p> <p>Clarify timelines for submission and introduce mandatory clearance certificate from regulatory authority to complete surrender.</p> <p>New Provision:</p> <p>"A licensee shall not be deemed to have surrendered a license until a</p>	<p>Rationale / Justification</p> <p>Ensures finality and regulatory closure and surrender protocols which require regulator certification of closure.</p>

		formal clearance certificate is issued by the relevant regulatory authority, confirming discharge of all liabilities and obligations under this Act.	
Section 17(1)(c)	The arrangement to be made in respect of client assets.	<p>Proposed Amendment:</p> <p>Expand to specify independent auditor verification of client asset reconciliation.</p> <p>New Language: "...accompanied by an auditor-certified report on the reconciliation and transfer of all client assets..."</p>	Protects consumer funds and aligns with FATF's recommendations on safeguarding client assets during license wind-down.
Section 17(2)(b)	Authority may give directions to the licensee to protect the interest of the customers or members of the public.	Make protection of customers a mandatory responsibility during surrender. New Clause: "...shall issue specific protective directions to safeguard customer assets and interests during the wind-down process."	Reinforces a duty of care and increases regulator accountability,
Section 18(1)	Requires the regulatory authority to maintain a register of licensees.	<p>Add obligation to publicly publish a searchable and regularly updated online register.</p> <p>New Clause: "...and shall publish and maintain the register in a publicly accessible electronic format updated on a quarterly basis."</p>	Enhances transparency and market confidence; reflects digital disclosure and registry practices.
Section 18(1)(c)	Mentions date of issuance of the license.	<p>Include date of expiry, status of license (active, suspended, revoked), and any conditions attached.</p> <p>New Clause: "...including date of issuance, expiry, current status, and any material license conditions imposed."</p>	Improves regulatory transparency and investor due diligence; aligns with FATF emphasis on transparency in supervision.

Section 19(1)	A licensee shall not appoint a director, senior officer or other such person unless the person is fit and proper.	Proposed Amendment A licensee shall not appoint or retain a director, senior officer, beneficial owner, significant shareholder or key function holder unless that person is determined to be fit and proper in accordance with criteria prescribed by the regulatory authority and subject to ongoing assessment.	Ensures inclusion of beneficial owners and key functionaries, aligning with FATF Recommendations 10 and 26. Prevents circumvention through indirect control or shadow appointments.
Section 19(2)(a)	Probity, competence, experience and soundness of judgment.	Replace with: “the person’s integrity, competence, professional conduct, decision-making capacity and record of regulatory compliance.”	Broadens scope beyond “probity” to encompass decision-making, ethics, and regulatory history.
Section 19(2)(c)	Education and professional membership as relevant.	Include language requiring evidence of continuing professional development or demonstrated knowledge of virtual asset services.	Brings focus to sector-specific expertise . Avoids licensing of nominal professionals with no actual grasp of blockchain, crypto, or cyber risk issues.
Section 19(2)(e)	Past dishonesty, malpractice, misconduct, bankruptcies.	Expand to include sanctions for AML/CFT violations, tax evasion, and disqualification from other regulatory jurisdictions.	FATF explicitly requires jurisdictions to exclude actors with AML/CFT offences or reputational risk from financial licensing. Ensures cross-border alignment and mitigates regulatory arbitrage.
Section 19(2)(f)	Contravention of any law with respect to virtual assets.	Broaden to include contraventions of data protection, cybersecurity, financial services or consumer protection laws in Kenya or any jurisdiction where the person has previously operated.	cross-jurisdictional scrutiny and ensures individuals with questionable records in other states are not able to act locally under a new entity
Section 19(2)(g)	Financial standing integrity.	Clarify to: “the person’s financial soundness, solvency status, ability to meet financial obligations, and absence of unmitigated financial distress or credit risk.”	Precision in language ensures this clause is enforceable. Focuses on both current and historical financial responsibility, preventing financial risk to client assets.
New Clause	(Not currently in the Bill)	(h) has not been the subject of adverse regulatory findings or public sanctions related to financial services, digital assets, or technology governance in the past 10 years.	Proactive inclusion of regulatory history requirement is crucial for public trust and market stability. FATF promotes exclusion of persons who could pose systemic reputational risk.

New Clause	<i>(Not currently in the Bill)</i>	(i) fit and proper assessments shall be ongoing and subject to regulatory review upon any material change in control, ownership, or operational responsibilities.	Brings the provision in line with ongoing due diligence norms under FATF Rec. 26. Removes false comfort of once-off clearance. Ensures bad actors can be removed even post-licensing.
20(1)	“A virtual asset service provider shall maintain a physical office in Kenya where its business activities are carried out.”	Replace with: “A virtual asset service provider shall maintain a principal place of business in Kenya, which may include a physical or virtual office that enables effective regulatory oversight.”	The current provision rigidly mandates a physical office, which is increasingly outdated for digital-first or decentralized financial services. Many VASPs operate globally with cloud infrastructure and minimal local footprint. Requiring a physical office increases cost and stifles innovation. A modernized definition accommodates innovation while ensuring accountability.
New Sub-Clause	—	“A virtual asset service provider shall appoint a compliance officer or authorized representative resident in Kenya, responsible for regulatory liaison and ongoing compliance.”	Introducing a compliance officer or resident agent ensures effective local engagement and supervisory access, without burdening the VASP with real estate overheads. This aligns with best practices under the FATF Recommendations (R.15 & R.26) responsible person framework. It balances regulatory oversight with operational flexibility.
21(1)	A licensee shall have a minimum of three directors, all of whom must be natural persons. A director shall not serve on more than two boards of licensees.	Expand to clarify: “...each director shall be a fit and proper person and collectively, the board shall demonstrate expertise in finance, technology, compliance, and risk management.”	While the clause establishes a basic governance floor, it lacks specificity around qualifications or diversity of expertise. Best practice includes “fit and proper” assessments and collective board competence. Limiting board seats promotes focus, but guidance should mandate board composition relevant to virtual asset risk profiles.
21(3)(a-e)	Lists criteria for assessing prudence: legal compliance, adherence to regulatory guidance, adequate capital, sound accounting, and insurance coverage.	Add a new clause (f): “has implemented an internal control framework, including independent compliance and audit functions appropriate to the size and complexity of the business.”	The current list is strong but misses internal control mechanisms and oversight structures. Supervisory regimes require not just financial and legal compliance, but robust risk governance architecture, including independent compliance/audit roles. Internal control frameworks are key to resilience and regulatory trust.
22(1)(a-c)	Prohibits mixer/tumbler services, misleading conduct, and mandates diligence in service delivery.	Add a new paragraph: “(d) maintain mechanisms to detect, prevent and report suspicious activities, including red flags for anonymity-enhancing tools or obfuscation techniques.”	This section rightly targets high-risk anonymity tools. However, it lacks a proactive monitoring obligation. FATF’s Guidance on Virtual Assets and VASPs (June 2023) stresses the importance of monitoring and reporting tools, not merely prohibition. Emphasize

			market abuse prevention. Kenya must move beyond moral framing (integrity) to systems-based enforcement.
22(2)	Offence and penalty provision.	Add: "...and shall be subject to both criminal and administrative penalties, proportionate to the severity of the breach and potential for consumer or systemic harm."	The enforcement clause lacks proportionality and gradation. digital finance laws distinguish between minor breaches and systemic misconduct, applying tiered sanction models. Kenya should incorporate a graduated penalty matrix to avoid binary enforcement.
23(1)	Requires compliance with capital, solvency, and insurance obligations.	Add: "...as determined by the regulatory authority in accordance with the risk profile, business model, and customer base of the licensee."	While sound, this clause would benefit from tying capital and solvency requirements to risk-based supervision principles, consistent with FATF R.15 and IOSCO Objectives. Adopt proportionality in prudential thresholds. Kenya must avoid fixed thresholds that ignore scale or risk class.
24(1)(a–c)	Requires conflict of interest policies covering licensee–client, licensee–third party, and intra-client relationships.	Add: "...and ensure that these policies include disclosure obligations, escalation protocols, and regular internal audits to review compliance."	Merely requiring policies is insufficient. Emphasize disclosure and mitigation. There should be enforceable procedures, not vague assurances. Effective governance demands traceable accountability.
24(2)	Enforcement clause.	Add: "...including revocation of license where conflicts materially harm client interests or market integrity."	Strengthens regulatory response options. Aligns with FATF and IOSCO principles on governance and fiduciary responsibility. Severe conflict breaches should be treated as grounds for license suspension or termination.
25(a–b)	Honest service delivery and maintenance of capital requirements	Clarify: "...in a manner that promotes fair market practices and protects clients from misrepresentation or exploitative terms."	These clauses reiterate foundational principles. However, 'honesty' and 'fairness' require clearer market conduct guidance on consumer protection.
25(c)	Manage actual and potential conflicts of interest	Reference to Section 24 for alignment	Redundancy risk exists. Better to cross-reference and consolidate. Ensure this clause invokes structured conflict resolution, not just vague intent.
25(d)	Adequate technological, financial, and human resources	Add: "...consistent with the scale, complexity, and risk profile of the services offered."	Mirrors risk-based resource allocation standards. Ensures scalability, not blanket standards.
25(e)	Full AML/CFT compliance	Add: "...including periodic risk assessments and transaction monitoring systems tailored to the nature of the VASP's operations."	Aligns with FATF Travel Rule. This should include digital KYC and ongoing surveillance protocols.

25(i–j)	Data governance and truthful marketing	Specify compliance with Kenya’s Data Protection Act and add: “...adhering to sectoral consumer data handling norms.”	Anchors VASPs within the Kenyan legal data sovereignty framework, ensuring harmonization with non-sectoral laws.
25(k–l)	Business continuity, disaster recovery, and customer complaint handling	Add: “...and demonstrate testing of business continuity plans at least annually; complaint mechanism must include escalation and resolution timelines.”	Moves this from policy presence to active governance. FCA and ASIC require testing of continuity plans and complaints dashboards.
25(m)	Whistleblower protection	Add: “...in accordance with the Whistleblower Protection Act (when enacted) or globally accepted standards.”	Reinforces alignment with expected future Kenyan law or fallback to OECD/UNODC frameworks.
25(n–o)	Market abuse and consumer education	Add digital asset literacy obligations and reporting thresholds for suspicious market conduct	Leverages and aligns with IOSCO principles on market transparency and consumer education.
25(p–q)	Employee legal compliance and staff competence	Include requirement for continuous professional training (CPT) annually	Embeds lifelong compliance competency, ensuring staff are up to speed with evolving threats.
25(r)	Due diligence on virtual assets	Specify pre-offer disclosures and issuer risk scoring	Kenyan VASPs should offer clarity on token utility, risks, and issuer solvency.
25(s)(i–v)	Vetting persons associated with the VASP	Add: “...and maintain documentation evidencing due diligence for each associated party.”	Documentation is critical to demonstrate compliance during audits.
29	29. (1) A licensee shall have appropriate and effective cyber security measures as prescribed or as provided for under the Computer Misuse and Cybercrimes Act	Replace Computer Misuse and Cybercrimes Act with Data Protection Act 2019	Computer Misuse and Cybercrimes Act does not prescribe cyber security measures only offences for abuses. The Cyber security measures are in Data protection Act and regulations.
30(1–3)	Requires annual audited financial statements by an approved auditor, submitted within 3 months after financial year end.	No changes to these subsections. However, insert a new Section 30A immediately after Section 30: “30A. System Audit Requirement: (1) A licensee shall, at least once every two years, commission a system audit by a certified IT auditor to assess its digital infrastructure, data security, transaction integrity, cybersecurity preparedness, and operational resilience.	The current law mandates financial audits but is silent on system and cybersecurity audits—a critical oversight in the context of virtual asset services, which are entirely tech-driven. Require IT and cybersecurity audit frameworks. This proposed Section 30A introduces a proportionate, risk-aligned requirement that ensures VASPs maintain secure infrastructure and are not exposed to unmonitored digital threats. It also allows the regulator

		<p>(2) The system audit report shall be submitted to the regulatory authority within 30 days of its completion.</p> <p>(3) The regulatory authority may issue guidelines on the scope, methodology, and frequency of such audits based on the licensee’s risk profile.”</p>	to tailor audit expectations based on the complexity and risk classification of the licensee.
31(1–4)	Requires appointment of a CEO who is fit and proper, with regulatory approval prior to designation.	Add to subsection (2): “...and shall possess demonstrable experience in digital finance, risk management, compliance, or related fields, proportionate to the size and complexity of the licensee.”	<p>The ‘fit and proper’ test is vague without sector-relevant competence indicators.</p> <p>Apply sector-specific criteria for executive roles in crypto/virtual asset service firms. Including domain-relevant expertise ensures competent leadership and reduces risk of mismanagement.</p>
33(2)(a–i)	Enumerates supervisory powers: vetting, inspections, document production, sanctions, and guidance issuance.	Add new clause (j): “require licensees to implement and periodically test AML/CFT risk assessment tools and transaction monitoring systems suited to virtual asset risks.”	The listed powers are strong but lack emphasis on technology-enabled compliance. Require automated screening, wallet analysis, and real-time monitoring for VASPs. Adding a system-testing power supports tech-enabled enforcement.
34(1–2)	Prohibits officers, agents, or employees from breaching AML/CFT rules. Violations attract criminal penalties.	Add to 34(1): “including failure to file suspicious transaction reports, failure to monitor high-risk wallets, and deliberate obfuscation of transaction trails.”	Adds specificity to actionable misconduct. Emphasize liability for both acts of commission and omission, particularly around suspicious activity reporting (SAR), PEP screening, and pseudonymous risk management. Clarity also enhances enforcement effectiveness.
35(2)	Bars natural persons from issuing assets from Kenya.	Reframe: “No natural person shall, in their personal capacity, issue or promote a virtual asset unless done through a licensed entity or legal person approved by the regulatory authority.”	Instead of a blanket ban, this amendment allows natural persons to operate through regulated vehicles, enhancing legitimacy while enabling innovation similar to Dubai VARA and UK FCA approaches.
35(3–4)	Issuers must apply for approval to issue or promote virtual assets in/from Kenya.	Add a reference to eligibility criteria: “...shall comply with eligibility criteria, disclosure obligations, and consumer protection requirements prescribed by the Authority.”	There’s a need to introduce a clear, risk-tiered framework for different asset classes (e.g., stablecoins vs. utility tokens). This enhances regulatory clarity and investor protection.

35(5)(a–f)	Grants the regulatory authority power to object and impose remedial measures post-issuance if discrepancies or misconduct are discovered.	Add: “...the regulatory authority may suspend the issuance, require additional disclosures, or order restitution to affected parties.”	The current provisions are reactive but lack enforcement clarity. Empower regulators to suspend, fine, and compel restitution where token offerings are misleading or breach public interest. This addition enhances investor protection.
35(6)	Criminalizes submission of false or misleading information in an application.	Add: “...including the omission of material facts likely to affect an investor’s decision-making or the regulator’s risk assessment.”	Expands liability to omissions, aligning with materiality standards. Many fraudulent disclosures involve omission, not just falsehood.
36(1)	Empowers the regulatory authority to conduct compliance inspections and investigations.	Add: “...including the power to enter premises, access digital systems, request transaction records, and engage third-party experts where technical assessment is required.”	Investigation authority must be explicit and digitally capable. As VASPs rely heavily on software systems, the regulator must be empowered to inspect code repositories, system logs, wallet activity, and algorithmic controls.
36(5)	Criminalizes supplying false or misleading information during an investigation.	Add: “including information supplied digitally or through third-party service providers.”	Expands the scope to cover API-based submissions, outsourced KYC vendors, and any digital onboarding/transaction data. Aligns with modern digital asset compliance contexts.
36(6)	Enables enforcement action for failure to comply with lawful regulatory requests.	Add: “...including, but not limited to, enhanced inspections, suspension of business activities, financial penalties, or license restrictions.”	Reinforces regulatory teeth. Broadens the range of possible sanctions beyond general enforcement under Section 40.
39(1)(c)	Allows the regulatory authority to summon persons for questioning.	Add: “...including by digital means such as secure video conferencing, where physical presence is impractical.”	Modernizes the provision to reflect digital-first compliance environments. Many regulatory authorities globally accept virtual hearings or testimony under secure protocols. This is especially vital when dealing with decentralized teams and foreign-based operators.
39(2)(a)	Requires production of documents in custody of senior officers or related persons.	Add: “...including digital records, encryption keys, access logs, and backup files relevant to operations of the licensee.”	This expands the clause to recognize the critical role of digital infrastructure in VASP governance and ensures the regulator has access to relevant tech-layer evidence.
39(2)(c)	Permits the regulator to direct specific actions during investigations.	Clarify: “...including the temporary suspension of services, wallet freezing, or internal access restrictions as reasonably required.”	Makes this clause operationally relevant by explicitly identifying intervention powers critical in the prevention of further harm or asset flight during ongoing investigations.
Section 39(3)	Allows regulator or their agent to copy or extract information.	Allows regulator or their agent to copy or extract information.	Allows regulator or their agent to copy or extract information.

Section 39(4)	Allows regulator to enter premises to obtain documents if needed.	Add: "...including digital premises such as data centres, server access locations, and remote storage environments under the control of the licensee or its agents."	Necessary to update the understanding of "premises" to include digital environments for effective enforcement in a borderless, digital-native space.
Section 39(5)	Defines connected persons for investigation purposes.	Add: "...or has had material influence, access, or oversight over digital systems, wallets, platforms, or protocols used by the licensee."	Broadens the scope beyond equity/shareholding to cover tech and ops influencers (e.g., outsourced CTOs, developers, third-party custodians).
40(1–2)	Grants the authority power to take administrative enforcement action for violations, including warnings, remedial directions, directives, and restrictions.	Add: "The authority shall maintain an enforcement register accessible to the public summarizing enforcement actions taken, subject to confidentiality under Section 43."	This amendment aligns with transparency principles where public enforcement registers deter repeat offenses and inform counterparties of risk.
40(2)(d–e)	Provides for suspension/revocation of licenses and initiation of investigations.	Add: "The licensee shall be given reasonable opportunity to respond prior to any revocation or suspension, unless urgent action is needed to prevent imminent consumer harm."	Ensures procedural fairness (audi alteram partem) while retaining the ability for swift action.
40(2)(f)	Sets administrative penalties: KES 3M for individuals, KES 10M for companies.	Adjust upward for inflation and add proportionality clause: "...or such higher amount as commensurate with the economic gain from the violation or harm caused to the public."	Introduces risk-based penalties, ensuring fines are not treated as the cost of doing business based on FATF's proportionality principle.
40(3)	Lists factors considered when determining enforcement action.	Add: "...including cooperation with investigations, voluntary disclosures, and implementation of compliance remediation plans."	Codifies incentives for cooperation and post-breach behavior, aligning with OECD guidance on cooperative enforcement.
41(1–3)	Categorizes fines and imprisonment terms for different offences, scaled by severity and whether committed by individuals or companies.	Add to each category: "...and the Court may, in addition, order disgorgement of profits, restitution to affected parties, or disqualification from holding office in a regulated entity."	Introduces reparative justice and market integrity measures. Restitution is critical in VASP markets where user losses can be massive.
Section 42 – Liability of	Holds directors, senior officers, partners, or employees liable for	Add: "The burden shall rest on the individual to demonstrate absence of	Shifts this into a "reverse burden" model similar appropriate for high-risk sectors like crypto. Promotes

Individuals for Organizational Offences	authorizing, permitting, or aiding an offence committed by the licensee.	knowledge or that reasonable steps were taken to prevent the offence.”	individual accountability and proactive risk management.
43(1)	Prohibits the regulatory authority or its agents from disclosing any information or documents obtained in the course of their duties.	Add: “...except in cases where disclosure is required to protect market integrity, prevent systemic risk, or inform other regulatory or supervisory bodies in Kenya under formal MoUs.”	Aligns with FATF Recommendation 40 and global practice where regulatory cooperation and information sharing are essential to prevent regulatory arbitrage and enable cross-border supervision. This ensures confidentiality is not a barrier to effective oversight.
43(2)(a–d)	Provides exceptions for disclosure under court orders, consent, anonymized statistical data, or legal requirements (e.g., AMLA, MLAA).	Add to (b): “...including digital consent mechanisms that are auditable and attributable to the individual or entity giving such consent.”	Reflects the digital-first nature of VASPs where consent may be logged electronically. Auditable digital consent trails are standard under GDPR, Kenya’s Data Protection Act.
44(2)	Gives the appeal body power to confirm, vary, revoke decisions and make appropriate orders.	Add: “...including ordering interim relief or suspending enforcement action until final determination.”	Prevents irreversible damage pending appeal. Aligned with judicial review principles and right to remedy provisions.
Section 46 – Protection from Liability	Shields regulators from legal action when duties are performed in good faith.	Add: “...provided such acts are not grossly negligent, reckless, or in willful disregard of statutory obligations.”	Introduces balanced immunity. Mirrors judicial precedents, CBK Act, and international public law norms that permit challenge where egregious failure exists.