BANK OF BOTSWANA

STRATEGIC PLANNING AND RISK MANAGEMENT DEPARTMENT

FINTECH ANALYTICAL ASSESSMENT FRAMEWORK

Produced by the
Botswana National Fintech Working Group

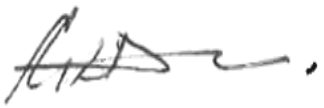
Foreword

The Botswana Fintech Landscape Mapping survey initially conducted in 2022 and refreshed in 2024 established the significant presence of fintech activities in Botswana. The survey identified fintech activities in operation within the local financial services sector, technologies driving the provision of the fintech services, and public policies that have been instituted or need to be established to facilitate and govern the safe and secure provision of fintech services in Botswana. These findings informed the development of this Fintech Analytical Assessment Framework, whose objective is to guide identification and regulation of fintech activities, identification and management of risks inherent in fintech services, as well as promotion of legal certainty for emerging fintech activities not covered by existing legal frameworks.

The Bank of Botswana (the Bank) guided by its role in the supervision and oversight over the National Payment System, and to generally ensure financial stability, motivated the establishment of the National Fintech Working Group, with the purpose to provide strategic direction and an integrated approach towards the safe and orderly adoption, regulation, and oversight of fintech developments across the local financial services industry. Membership of the National Fintech Working Group draws from Government and key stakeholders in the financial services industry to embrace market players in the fintech ecosystem. The development of the Fintech Analytical Assessment Framework was a key project for the National Fintech Working Group.

Furthermore, the Bank has established a Digitalisation and Innovation Hub (DIH), with the mandate to monitor local and global fintech developments with a view to timely inform the requisite regulatory policy responses and facilitate orderly adoption of emerging technologies by the financial services sector. This mandate encompasses provision of guidance on navigation of the regulatory landscape for fintech products and services. The Fintech Analytical Assessment Framework provides a guide in this regard.

The Bank and other National Fintech Working Group stakeholders acknowledge that the global fintech industry is constantly developing and as such, there will be a need to keep abreast with global fintech developments and realign guidance as and when necessary. The Bank in collaboration with stakeholders remains committed to promoting innovation in financial services and the development of the financial services infrastructure while maintaining the safety, integrity, and stability of the financial system.



Cornelius K Dekop
Governor
BANK OF BOTSWANA.

Acknowledgements

The Fintech Analytical Assessment Framework was developed through a consultative process, coordinated by the National Fintech Working Group. The National Fintech Working Group comprises the following organisations: Bank of Botswana (provides chairmanship); Ministry of Finance; Non-Bank Financial Institutions Regulatory Authority (NBFIRA); Botswana Communications Regulatory Authority (BOCRA); Ministry of Trade and Entrepreneurship; Ministry of Communications and Innovation; Bankers Association of Botswana (BAB); Financial Intelligence Agency (FIA); Botswana Digital and Innovation Hub (BDIH); Botswana Unified Revenue Service (BURS); Competition and Consumer Authority; Fintech Association of Botswana; Business Botswana; and Botswana Fibre Networks.

Additionally, we express our sincere gratitude to AfricaNenda[1] for the valuable quality review of the Fintech Analytical Assessment Framework and insightful input.

[1] AfricaNenda is an Africa-based, Africa-led nonprofit organisation that works to accelerate the development and adoption of inclusive instant payment systems across the continent, with a view to remove barriers to the deployment and scale of inclusive instant payment systems in Africa, to accelerate universal access to digital payments and financial inclusion.

Disclaimer

The information in this document is strictly for guidance purposes only and neither constitutes a licensing framework for the various fintech products and services nor legal advice. Consult with relevant regulatory authorities for specific products and services as necessary.

GLOSSARY

AI	Artificial Intelligence
AML	Anti-Money Laundering
APIs	Application Programming Interfaces
ATM	Automated Teller Machine
BACH	Botswana Automated Clearing House
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
BISS	Botswana Interbank Settlement System
CBDC	Central Bank Digital Currency
CBR	Correspondent Banking Relationship
CFT	Counter Financing of Terrorism
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
CSD	Central Securities Depositories
CSDB	Central Securities Depository Botswana
CSP	Critical Service Provider
ELMI	Electronic Money Issuer
EPS	Electronic Payment Services
EU	European Union
FATF	Financial Action Task Force
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
GSC	Global Stablecoin
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IFT	Informal Funds Transfers
IOSCO	International Organisation of Securities Commissions
ISO	International Standards Organisation
IMF	International Monetary Fund
ML	Machine Learning
MNO	Mobile Network Operator
mPOS	Mobile Point of Sale
MTO	Money Transfer Operators
MVTS	Money or Value Transfer Services
NCSS	National Clearance and Settlement
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OTC	Over the Counter
PCI DSS	Payment Card Industry Data Security Standard
PFMI	Principles for Financial Market Infrastructures
PI	Payment Institution
PSD2	Payment Services Directive 2 of the European Union
PSP	Payment Service Provider
SIPS	Systemically Important Payment System
SME	Small Medium Enterprises
VA	Virtual Asset
VASP	Virtual Asset Service Provider

TABLE OF CONTENTS

1. INTRODUCTION

The Bank for International Settlements (BIS) Financial Stability Board (FSB) defines fintech as "technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services" (FSB 2017). The FSB guidance on the regulatory treatment of fintech prescribes the "same activity, same risks, same regulation" or "same activity, same risks, same regulatory outcomes" guiding principle for the regulation of fintech services. This underlying principle requires that there should be an effective regulatory framework for fintech driven services. Further, the guiding principle requires that the regulatory framework for fintech should ensure that fintech services are subjected to comprehensive regulation that is proportionate to the risks that fintech activities pose to the stability and integrity of the financial system and create a level playing field for both incumbent financial services and emerging fintech services. It is also recommended that the fintech regulatory framework should harness potential benefits of fintech enabling technologies to broaden provision of financial services and deepen financial inclusion.

Therefore, this Fintech Analytical Assessment Framework has been developed for the financial services sector in furtherance of the Botswana financial services regulatory authorities' mandate of maintaining the stability of the financial system as well as the development and enhancement of the National Payment System (NPS) in line with the Fintech Development Pillar of the Payment System Vision and Strategy 2022 - 2024. This follows the fintech landscape mapping survey carried out across the financial services sector in 2022, whose findings suggested significant presence and growth of fintech services in Botswana. Having observed the increasing adoption of fintech services by the financial services sector and the growing integration of banks and other non-bank financial institutions through fintech driven partnerships, it has become expedient that the financial services sector should establish an appropriate framework to guide regulation of fintech services and mitigation of fintech related risks to the financial system.

Pursuant to their role in financial sector development, and in view of the interconnectedness of fintech driven services to both the broader financial system and the NPS, the Botswana financial services regulatory authorities are committed to facilitating adoption of beneficial international best practice standards in the financial services sector with due cognisance given to fintech related risk management and applicability in the Botswana environment. Therefore, this Fintech Analytical Assessment Framework is issued to guide regulation of fintech services, foster innovation in financial services, and harmonise fintech related legal and regulatory frameworks.

2. OBJECTIVES

The objective of the Fintech Analytical Assessment Framework is to guide the Botswana financial services sector in:

(a) identification of fintech and related economic activities;
(b) licensing and designation of fintech activities for prudential supervision, regulation, and oversight;
(c) identification, analysis and management of emerging risks that may not be effectively addressed by existing legal and regulatory frameworks;

(d) promotion of legal certainty of emerging innovative fintech services through a transparent, comprehensive and sound legal framework for emerging fintech products and services as well as institution of appropriate policy responses to ensure payments stability, financial stability and monetary stability.

3. SCOPE

The scope of the Fintech Analytical Assessment Framework covers regulation of fintech activities offered by:

(a) the banking sector;
(b) the Electronic Payment Services/Money or Value Transfer Services (EPS/MVTS) sector, and
(c) the non-bank financial institutions sector with implications for both the broader financial system and the NPS as classified per the FSB Fintech Tree Conceptual Framework.

4. FINANCIAL SERVICES LEGAL AND REGULATORY FRAMEWORKS

In alignment with the FSB's "same activity, same risks, same regulation" or "same activity, same risks, same regulatory outcomes" guiding principle, regulation of fintech services in Botswana will build on existing legal and regulatory frameworks for incumbent financial services to accommodate emerging technologies and create a level playing field.

4.1. Banking and EPS/MVTS Sector Legal and Regulatory Framework

The banking sector regulatory authority's financial services supervisory and oversight powers for services impacted by fintech developments are established in the following laws:

(a) Bank of Botswana Act (CAP 55:01) as amended;
(b) Banking Act (2023) and Banking Regulations (2025), which regulate provision of banking services;
(c) Electronic Payment Services Regulations (2019), which regulates electronic payment/money or value transfer services (EPS/MVTS);
(d) National Clearance and Settlement Systems (NCSS) Act (CAP.46:06) and the NCSS Regulations (2005), which regulate clearing and settlement systems;
(e) Financial Intelligence Act (2022), the Financial Intelligence Regulations (2022), and the Financial Intelligence (Implementation of UNSCR) Regulations (2022), for Anti-Money Laundering/Counter Financing of Terrorism and Proliferation (AML/CFT) risk-based supervision;

An all-encompassing payment systems law, the National Payment Systems law is currently being developed to replace the NCSS Act, with an objective of facilitating the regulation of payment systems and payment service providers (PSPs) inclusive of emerging fintechs to maintain a safe and efficient payment system, the integrity of the monetary system, safeguard financial stability, and protect consumers with regards to non-fiat currency payments that entail credit risks.

4.2. Non-Bank Financial Institutions Sector Legal and Regulatory Framework

The Non-Bank Financial Institutions Regulatory Authority (NBFIRA)'s regulatory and oversight powers for services impacted by fintech developments are established in the following laws:

(a) NBFIRA Act (2023), which regulates Medical Aid Funds, Pawnshops, Finance and Leasing Companies, and all other Non-Bank Financial Institutions (NBFI's);

(b) Financial Intelligence Act (2022), the Financial Intelligence Regulations (2022), and the Financial Intelligence (Implementation of UNSCR) Regulations (2022), for Anti-Money Laundering/Counter Financing of Terrorism and Proliferation (AML/CFT) risk-based supervision;

(c) Virtual Assets Act (2025), and related Regulations, which regulate the sale and trade of virtual assets (VAs), licensing of VASPs and issuers of initial token offerings in Botswana, with primary focus on risks associated with virtual assets in the context of emerging business practices and technologies. VASPs include issuers of initial token offering, businesses that provide services related to virtual tokens; businesses that operate as payment service providers utilising virtual assets; businesses that operate as VASPs, including providing a distributed ledger technology platform which facilitates the exchange between virtual assets and fiat currency and exchange between one or more forms of virtual assets; or, businesses that participate in and provide financial services related to an issuer's offer or sale of a virtual asset as may be prescribed;

(d) Insurance Industry Act (2014), and the Insurance Industry Regulations (2019), for regulation of Insurers, Reinsurers, Insurance Brokers, and Insurance Agents;

(e) Securities Act (2014) and Securities (Amendment) Act (2023) and the Securities Businesses Regulations, 2017 for regulation of the capital markets, comprising Asset Managers, Securities Infrastructure Business, Securities Brokers, Investment Advisors, Custodians, and Market Makers;

(f) Collective Investment Undertakings (CIUS) Act (2021), for regulation of Collective Investment Undertakings (CIUs), Investment Companies, Trustees, and Management Companies; and the

(g) Microlending Regulations (2012), for regulation of microlenders.

4.3. Other Supporting Legislations

Other supporting legislation whose focus is on public policy objectives of consumer protection, cyber and data security, include the following:

(a) Consumer Protection Act (CAP 42:07);
(b) Data Protection Act (2024);
(c) Electronic Records (Evidence) Act (2014);
(d) Electronic Communications and Transactions Act (2014);
(e) Bills of Exchange Act (CAP 46:02); and

(f) Competition Act (2018).

5. THE FOUR STEP FINTECH ANALYTICAL ASSESSMENT FRAMEWORK

For purposes of this Fintech Analytical Assessment Framework and guidance, the FSB definition of Fintech is adopted, wherein Fintech is defined as technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services. The Fintech Analytical Assessment Framework, which provides guidance on regulation of fintech activities and strengthening their supervision in Botswana is organised around four key steps as follows:

(a) **Step 1** - examines if an underlying economic activity is considered a fintech activity;

(b) **Step 2** - determines if the fintech activity and the entity offering the activity require licensing;

(c) **Step 3** - analyses risks to determine existence of any risks that are not effectively addressed by the existing regulatory framework, including risks associated with funds protection, financial integrity, cyber and data security, access to payment systems, and interoperability;

(d) **Step 4** - promotes legal certainty through development of a transparent, comprehensive and sound legal framework for fintech services and institution of appropriate policies to ensure payments stability, financial stability and monetary stability.

The rest of this Framework is organised as follows:

(a) Subsection 5.1 of this document provides guidance on the identification of services that are considered fintech activities;
(b) Subsection 5.2 provides guidance on licensing and designation of fintech activities;
(c) Subsection 5.3 examines risks occasioned by fintech activities and the management thereof;
(d) Subsection 5.4 provides guidance on provision of legal certainty; and
(e) Section 6 provides guidance on operation of Innovation Facilitators.

The Bank in its facilitative role, through the National Fintech Working Group, will coordinate the development of fintech enabling policies in collaboration with other key stakeholders to address regulatory gaps and address fintech related technology risks. Execution of the four (4) fintech assessment steps culminates into regulatory sandboxing in the case of startups and emerging innovative fintech activities that are not covered by existing legal and regulatory frameworks or issuance of a licence for fintech services that meet all licensing requirements.

Figure 1 provides a schematic conceptual view of the 4-Step Fintech Analytical Assessment Framework.

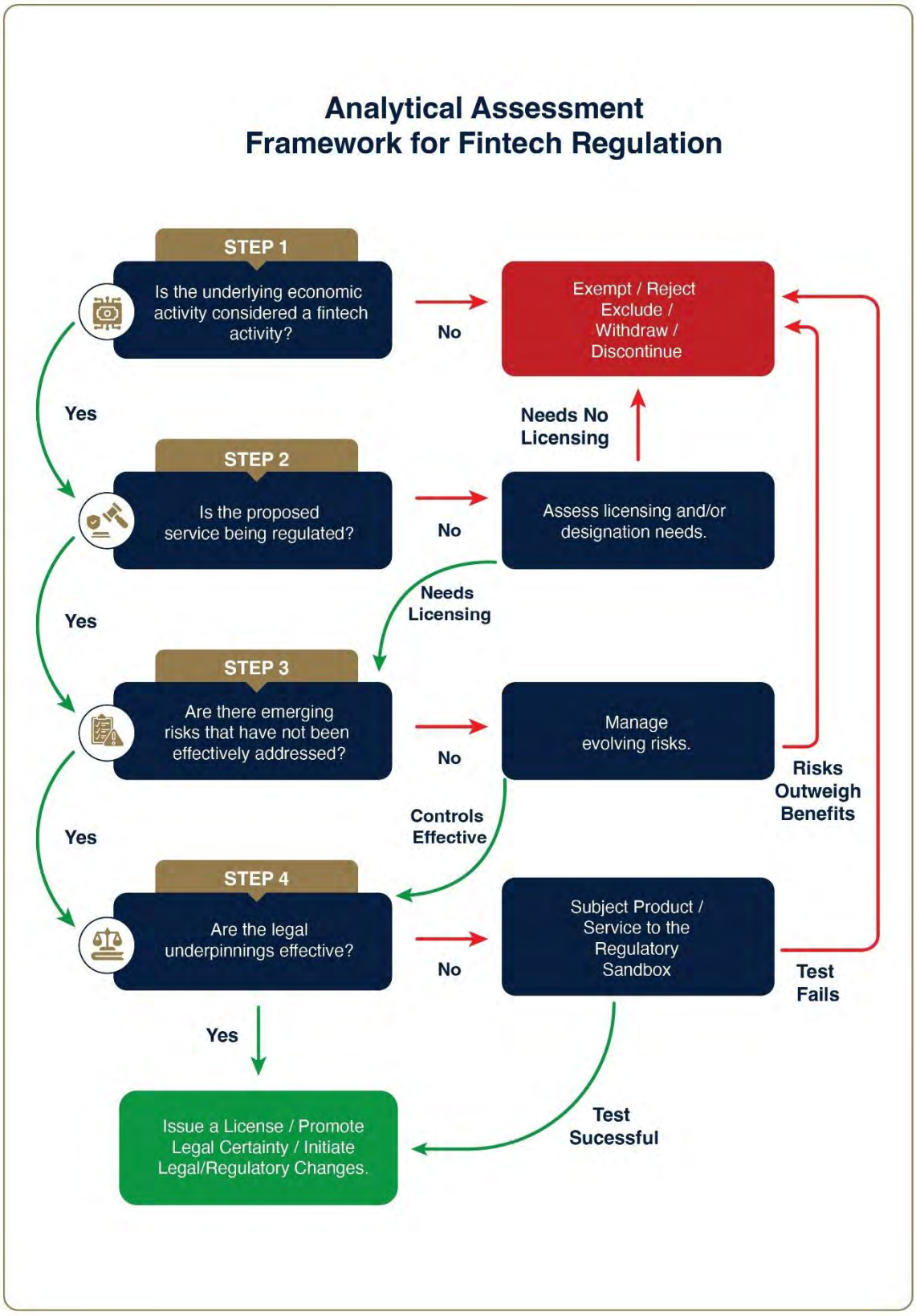


Figure 1 Analytical Assessment Framework for Fintech Regulation

5.1. STEP 1: IDENTIFICATION OF FINTECH ACTIVITIES

The following financial services functions that comprise the financial services sector in Botswana will form the basis for identification and appropriate categorisation of emerging fintech driven economic activities based on the primary economic function they provide:

(a) Deposit and Lending;
(b) Capital Raising;
(c) Asset Management;
(d) Insurance Services;
(e) Payments, Clearing and Settlement; and
(f) Virtual Assets.

Identification and classification of fintech activities will be in line with the below nine (9) fintech categories that serve the above six (6) financial services functions as follows:

(a) Digital Banking Services;
(b) Fintech Balance Sheet Lending Services;
(c) Loan Crowdfunding Services;
(d) Equity Crowdfunding Services;
(e) Robo-Advisory Services;
(f) Digital Payment Services;
(g) Electronic Money Issuance;
(h) InsurTech Business Models; and
(i) Virtual Assets Related Financial Services.

5.1.1. Digital Banking Services

In alignment with the FSB definition, digital banks will be defined as deposit-taking technology-enabled business models that are innovative alternatives to traditional brick-and-mortar banks. Identification of digital banks will be based on the following key differentiating features:

(a) **Establishment** - either a legacy bank that has entirely moved to digital/internet services with no physical branches or a new bank that operates fully online with no physical branches;

(b) **Physical Presence** – operating entirely online with no physical presence and delivering banking services primarily through electronic channels instead of physical branches;

(c) **Ownership** - autonomous or part of a larger traditional bank's digital service;

(d) **Partnerships** - having links with their parent organisation or collaborating with third parties;

(e) **Product Offering** - offering traditional banking products such as savings accounts, checking accounts, loans, credit cards, mortgages, and investment opportunities or access to financial advisors with a modern or digital dimension;

(f) **Technology and User Experience** - relying extensively on technology to supply services and enabling customers to manage their money conveniently from their smartphones or computers;

(g) **Personalised Service** - leveraging advanced technologies such as artificial intelligence and machine learning to provide personalised financial advice and recommendations tailored to each customer's unique needs;

(h) **Convenience** - products and services are accessible through user-friendly mobile apps and websites that allow customers access to their accounts anytime and anywhere;

(i) **Emphasis on Security** – heavy investment in robust cybersecurity measures to protect customer data from unauthorised access or breaches, use of encryption techniques, multi-factor authentication, and continuous monitoring systems to ensure the safety of transactions and personal information; and

(j) **Efficiency and Cost-effectiveness** - and reducing overhead costs through elimination of the need for physical branches, better interest rates on savings accounts, and lower fees on transactions compared to traditional banks.

5.1.2. Digital Payments Services

Digital payment services will be defined as technology driven financial services that facilitate payment transactions by transferring money, virtual assets, clearing or settling balances digitally, without the use of physical money (FSB). This shall involve digitally channelling funds/virtual assets from payers to payees by either handling payers' money/virtual assets or initiating payment orders on behalf of payers with respect to transaction accounts held at other financial institutions. Key features for identification of digital payment services shall be as follows:

(a) **Delivery Channel -** transactions facilitated digitally, online, over blockchain based platforms, or through other electronic media or device without any transfer of cash in the physical form;

(b) **Type of Service Providers** – banks and non-banks;

(c) **Type of Products** – online electronic payment systems; mobile payment apps e.g. Unstructured Supplementary Service Data (USSD); Point-of-Sale (PoS); mobile wallets, digital wallets inclusive of blockchain/DLT driven wallets, e-wallets; digital cards (credit, debit or prepaid card); contactless payments (QR based payments, contactless credit, debit, and prepaid cards) with near-field communication (NFC) technology, mobile wallets that use magnetic security transmission (MST) technology; and virtual assets;

(d) **Type of Service** – execution of payment transactions by transferring funds or virtual assets from payers to payees; initiation of payment transactions from the payer's account to the payee's account without handling any customer funds or virtual assets;

offering payment services by placing an overlay on existing payment infrastructures (e.g. Paypal, Calibra); and use of own proprietary standalone systems (eg Alipay, WeChat Pay); and

(e) **Digital Payments Ecosystem Key Components**[2] - payer, merchant/payee, a payment network which involves the payer's payment provider (the issuer) and the payee's payment provider (the acquirer), the payer's account, and the receiver's account.

5.1.3. Electronic Money Issuance (e-Money)

E-money issuance shall be defined as an electronic store of monetary value on a technical device or issuance of prepaid debt-like instrument that is issued upon receipt of funds for the sole purpose of facilitating payment transactions to entities other than the e-money issuer (FSB). The following features which constitute the e-money test shall be used to identify electronic money issuance services:

(a) **Storage** - the asset is stored electronically;
(b) **Storage Type** - hardware (chip card that requires no internet connectivity) or software that requires active network connection to enable transfers and payments;
(c) **Asset Type** – the asset is a representation of monetary value;
(d) **Identifiability of Issuer** - identifiable/anonymous;
(e) **Liability** - issuance of the asset creates financial liabilities of the issuer towards the asset equal to the funds received in exchange for the asset;
(f) **Purpose** – the asset is issued for the purpose of facilitating payment transactions;
(g) **Mode of Usage** - online/offline instruments;
(h) **Issuance** – the asset is issued on receipt of funds, and hence, the asset has a prepaid nature with no credit facility provided;
(i) **Interest/Benefits** - issuer does not pay interest or other benefits related to the length of holding the asset;
(j) **Acceptance** – asset is accepted not only by the issuer and/or network services providers and vendors but widely acceptable as a form of payment;
(k) **Exclusion** – is not excluded under the electronic communications exclusions; and
(l) **Type of electronic money** - e-cash, central bank digital currencies, and virtual assets;

5.1.4. Fintech Balance Sheet Lending Services

Balance sheet lending services will be defined as a type of fintech platform financing where credit activity is facilitated by non-bank lenders that use their own balance sheet to provide credit to borrowers through electronic channels (FSB). The following key features will be used for identification and classification of Fintech Balance Sheet Lending Services:

(a) Facilitation of credit activity by internet-based platforms and not commercial banks;
(b) Use of own balance sheet in the ordinary course of business to intermediate borrowers and lenders by relying on other sources, such as own capital or debt issuance;

[2] Includes Virtual Assets ecosystem components.

(c) Origination and retention of loans on platform's own balance sheet;
(d) Lending platform carries all the risk for losses;
(e) Lending platform undertakes credit risk analysis on borrowers;
(f) Lending platform provides funds to borrowers at a cost;
(g) Funds readily available for disbursement by the lending platform immediately upon loan application approval; and
(h) Lending platform collects funds from borrowers.

5.1.5. Loan Crowdfunding Services

Loan Crowdfunding Services will be defined as a type of fintech platform financing where lenders and borrowers are matched online (FSB). The following key identification features shall be used for identification and classification of Loan Crowdfunding Services:

(a) Facilitation of credit activity by internet-based platforms and not commercial banks;
(b) Activities are exclusive of balance sheet lending;
(c) Matching of borrowers with lenders facilitated by platform;
(d) Individual loan contracts are established between borrowers and lenders;
(e) Funds may be disbursed instantly or over a funding period;
(f) Platform does not engage in risk transformation; and
(g) The investor carries all the risk for losses.

5.1.6. Equity Crowdfunding Services

Equity Crowdfunding Services will be defined as a type of fintech platform financing where investors and investees are matched online (FSB). The following key platform features shall be used for identification and classification of Fintech Crowdfunding Services:

(a) Credit activity is facilitated by internet-based platforms and not commercial banks;
(b) Activities are exclusive of balance sheet lending;
(c) Platform facilitates matching of investors with companies that are desirous of investing (investees), enabling them to participate in the early capital raising activities of startups and other companies;
(d) Investors provide funding to private companies in exchange for equity;
(e) Individual loan contracts are established between investors and investees;
(f) Funds may be disbursed instantly or over a funding period;
(g) Platform does not engage in risk transformation; and
(h) The investor carries all the risk for losses.

5.1.7. Robo-Advisory Services

Robo-advisory[3] services will be defined as automated digital financial advice on investment products that is provided with no or limited human intervention and relies on technology to automate the client onboarding process and the generation of advice through algorithm-based tools (FSB). The following features shall be used for identification of fintech driven robo-advisory services:

[3] Examples include Wealthsimple, Wealthfront, Betterment, Ellevest, and Sofi Automated Investing etc

(a) **Delivery Channel** – provision of services automatically technology driven, involving use of algorithms for analysis of investment needs and generation of advice;
(b) **Type of Advice** – both scaled and comprehensive personalised financial advise;
(c) **Type of Advisor** – restricted, non-restricted, independent, non-independent, and fully automated;
(d) **Type of Product** - the applicability of regulations shall be on the basis of the product being a securities, insurance or banking product;
(e) **Type of Client** – individuals, retail, or legal entities;
(f) **Purpose of Investment** – all types of financial investments; and
(g) **Type of Activities Performed** – generation of advice, passing of clients' orders to brokers, execution of clients' orders on own platform, rebalancing clients' portfolios in line with the advice given, or managing clients' portfolios beyond rebalancing.

5.1.8. InsurTech Business Models

InsurTech business models will be defined as emerging technology-driven innovative models that facilitate (i) insurance distribution, such as comparison portals and digital brokers; and (ii) underwriting, such as mobile, on demand, usage-based or technology-enabled peer-to-peer and parametric insurance (FSB). InsurTech business models shall be categorised as follows:

(a) **Direct Insurers/Tied Agents**[4] - offer personalised, flexible, and cost-efficient packages with typically lower coverage and premiums. Such insurtech firms adopt technology innovations like Internet of Things (IoT) or Data Science, and their products can be easily purchased via a website or mobile app;

(b) **Underlying Technologies** - Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), Robotic Process Automation (RPA), Blockchain, Advanced Analytics (AA) and drones;

(c) **Insurance Management Solutions**[5] – shall be characterised by primary focus on convenient tracking and administration of insurance policies and contracts in one place;

(d) **Marketplaces/Aggregators**[6] – shall be characterised by online platforms with numerous insurance products that facilitate comparison of prices and terms by users;

(e) **Peer-to-Peer/Cashback Insurtech Solutions**[7] – shall be characterised by functionality that allows individuals to team up and club their premiums together to hedge against risk and derive benefits regarding premium proceeds; and

[4] Examples of Direct Insurers/Tied Agents include BIMA, Metromile, Trov, ROOT, Cuvva, and NEOS
[5] Examples of process-improvement insurtech products include FinanceFox, Brolly, Knip, Rentablo, and GetSafe
[6] Examples of Marketplaces/Aggregators include PolicyBazaar, CoverHound, Insurify, PolicyGenius, and Coverfox
[7] Examples of peer-to-peer /cashback insurtech models include Friendsurance, Guevara, Lemonade, Uvamo, and insPeer;

(f) **Sales, Marketing, and Engagement InsureTech Models**[8] – shall be characterised by provision of focused tools to industry-related third parties, including but not limited to brokers and insurers, mainly in the form of API or Software as a Business (SaaS) model to improve parts of the value chain, user experiences and facilitate fair pricing.

5.1.9. Virtual Assets Related Financial Services

Virtual assets related financial services will be defined as financial services that include creating, distributing, storing or exchanging virtual assets, using them for investment or payment purposes, or as reference in financial products. The following key features shall be used to identify virtual assets related financial services:

(a) **Asset Form** – it is a digital or electronic representation of value;

(b) **Asset Properties** – it may be transferred, stored and traded electronically;

(c) **Asset Function** – it may be used as a means of payment or exchange, store value or unit of account;

(d) **Underlying Technology** - distributed ledger technology (DLT);

(e) **Nature of the Issuer -** may be issued by non-regulated entities, regulated financial entities or the public sector;

(f) **Underlying Economic Function -** may be used as a means of payment or exchange ("payment tokens"); as a source of investment, giving holders rights and obligations ("security tokens"); and can also grant holders access to a current or future service ("utility tokens"). The underlying economic function shall be used to determine applicable regulatory frameworks; and

(g) **Underlying Assets** - may be unbacked or backed by fiat currency, commodities (eg precious metal), real estate or securities. The underlying asset shall be used to determine applicable regulatory requirements.

Enabling technologies underlying and driving the provision of fintech services, and facilitating innovation in the provision of financial services will be classified as follows:

(a) Application Programming Interfaces (API);
(b) Cloud Computing (CC)
(c) Artificial Intelligence (AI);
(d) Machine Learning (ML);
(e) Biometric Identification and Authentication (BIA), and
(f) Distributed Ledger Technologies (DLT).

The following enabling policies will form the foundation for the provision of fintech services and the necessary mitigation of technology related risks to the financial system:

[8] Examples of Sales, Marketing, and Engagement InsurTech Models include Zywave, Welltok, KASKO, CoVi Analytics, Zipari, Qover, Dynamis, LifeDrip, and Sureify.

(a) Digital Identification Policy;
(b) Open Banking Policy;
(c) Data Protection Policy;
(d) Cyber Security Policy; and
(e) Innovation Facilitators Policies.

Any economic activity that cannot be classified as a financial service or fintech activity in line with this Analytical Framework will be exempted or excluded from licensing in accordance with guidance detailed in this Framework.

5.2. STEP 2: LICENSING AND DESIGNATION OF FINTECH ACTIVITIES

Economic activities identified as fintech activities will be assessed to determine the need for licensing and designation. The regulatory treatment of fintech activities will follow the basic principle of "same activity, same risks, same regulatory outcomes" wherein if the economic function and purpose of a fintech activity are the same as a regulated financial service, then the fintech activity will be subject to the same regulatory frameworks on AML/CFT/CPF, securities trading, banking, payments, fund management, or financial infrastructure regulation unless specifically stated. Similarly, if a fintech firm or intermediary is engaging in activities that are by nature similar to those performed by regulated financial services providers or intermediaries, then such activities will be subjected to the same financial regulation unless specifically stated.

Regulatory responsibilities for fintech activities will have two distinct roles - prudential supervision and oversight. Prudential supervision will be focused on service providers while oversight will be focused on payment systems, critical service providers, payment instruments, and payment schemes.

The high-level licensing and designation process for the licensing of fintech services will be as follows:

(a) **Application** - applicant will submit business model to the regulatory authority;
(b) **Determination** – the regulatory authority will consider exemption, exclusion, threshold, and systemic importance;
(c) **Licensing** – the regulatory authority will consider full or limited licence or registration;
(d) **Designation** – the regulatory authority will consider systemic importance of business model and payment system; and
(e) **Eligibility** – the regulatory authority will consider access to payment, clearing, and securities settlement systems as well as settlement account policy, where applicable.

5.2.1. Licensing of Digital Banks

Regulation of digital banks will follow the "same activity, same risk, same regulatory outcomes" principle. Applicants for a banking licence with a fintech business model will be subjected to the existing legal and regulatory framework applicable to traditional banks with added technology specific policy requirements listed as follows:

(a) Bank of Botswana (Amendment) Act (CAP 55:01);
(b) Banking Act (2023);
(c) Banking Regulations (2025)

(d) Financial Intelligence Act (2022);
(e) Financial Intelligence Regulations (2022);
(f) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(g) Consumer Protection Act (CAP 42:07);
(h) Competition Act (2018);
(i) Data Protection Act (2024);
(j) National Financial Services Cyber Security Framework;
(k) Open Banking Policy;
(l) Artificial Intelligence/Machine Learning Policy;
(m) Application Programming Interface Guidelines;
(n) Cloud Computing Security Guidelines; and
(o) any other relevant legal instruments developed from time to time.

More specifically, digital banks will be assessed for compliance with the following specific requirements:

(a) Legal form and place of incorporation - applicant's incorporation in Botswana;
(b) Ownership structure/control – applicant controlled by Batswana and headquartered in Botswana;
(c) Track record in technology - an applicant's (or its parent group) track record in operating an existing business in the technology or e-commerce, provision of clear value propositions on how existing unmet or underserved needs will be served, and demonstration of existence of a sustainable digital banking business model;
(d) Fitness and propriety test on technology fields - suitability of members of senior management in terms of Information Technology competence, financial competence, fitness and propriety;
(e) Third party assessment of IT systems - assessment of technical infrastructure by independent third-party technology experts;
(f) Fitness and propriety test - suitability of shareholders (reputation and financial soundness of controlling shareholders);
(g) Long term sustainability of the business plan - existence of parent companies that are committed to and capable of supporting the digital bank;
(h) Minimum paid up capital - capital requirements, liquidity, and solvency arrangements in accordance with set minimum requirements;
(i) Sound risk governance frameworks - establishment of appropriate risk management controls for technology as prescribed by fintech enabling policies, operational, liquidity, and reputation risk;
(j) Structural organisation with respect to credit scoring and governance, IT related risks, outsourcing, data governance, and security;
(k) Consumer protection- compliance with consumer protection requirements;
(l) Requirement to foster financial inclusion;
(m) Compliance with ongoing regulatory requirements and exit plan - compliance with the same suite of ongoing prudential requirements applicable to incumbent banks as they relate to ongoing capital requirements, leverage liquidity requirements, anti-money laundering/combating the financing of terrorism and counter proliferation financing (AML/CFT/CPF), market conduct, data protection, and cyber security, and provision of a viable exit plan to facilitate an orderly wind-up if necessary; and
(n) Participation in the Deposit Insurance Scheme of Botswana.

5.2.2. Licensing of Digital Payment Activities and eMoney Issuance

Licensing of fintech driven payment services will be based on provision of any or a combination of the following types of activities:

(a) services enabling cash or digital tokens to be placed on a payment account as well as all the operations required for operating a payment account;
(b) services enabling cash or digital payment tokens withdrawals from a payment account as well as all the operations required for operating a payment account;
(c) execution of payment transactions, including transfers of funds or digital payment tokens on a payment account with the user's payment service provider or with another payment service provider;
(d) execution of direct debits, including one-off direct debits;
(e) execution of payment transactions through a payment card or a similar device;
(f) execution of credit transfers, including standing orders;
(g) issuance of payment instruments and/or acquisition of payment transactions;
(h) money remittances;
(i) payment initiation services;
(j) account information services; and
(k) execution of payment transactions where funds are covered by a credit line for a payment service user, which include:

    (i) execution of direct debits, including one-off direct debits;
    (ii) execution of payment transactions through a payment card or a similar device; and
    (iii) execution of credit transfers, including standing orders;

Fintech driven payment services will be categorised as below and assessed in line with applicable licensing requirements per the applicable legal and regulatory frameworks:

(a) account issuance;
(b) e-money issuance;
(c) remittances (domestic funds transfer and cross-border funds transfer);
(d) merchant acquisition (and/or payment gateways); and
(e) virtual asset payment service (digital payment tokens).

Emerging fintechs that provide digital payment services and e-money issuance as categorised above will be assessed for licensing and designation by being subjected to requirements of the following laws and regulations with added technology specific policy requirements as may be appropriate:

(a) Bank of Botswana (Amendment) Act (CAP 55:01);
(b) Banking Act (2023)
(c) Banking Regulations (2025);
(d) National Payment System Law (Drafting underway)
(e) Electronic Payment Services Regulations (2019);
(f) National Clearance and Settlement Systems (NCSS) Act (CAP 46:06);
(g) NCSS Regulations (2005);
(h) Financial Intelligence Act (2022);
(i) Financial Intelligence Regulations (2022);

(j) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(p) Consumer Protection Act (CAP 42:07);
(q) Data Protection Act (2024);
(r) National Financial Services Cyber Security Framework;
(s) Open Banking Policy;
(t) Application Programming Interface Guidelines;
(u) Cloud Computing Security Guidelines;
(v) Artificial Intelligence/Machine Learning Policy;
(w) Distributed Ledger Technology Guidelines;
(x) Competition Act (2018); and
(y) any other relevant legal instruments developed from time to time.

Activities such as cash, paper-based payment instruments (drafts, vouchers, postal money orders), and ATM cash withdrawal services, among others, shall be exempted from licensing as fintech driven digital payment services under this Framework.

5.2.3. Fintech Financing Platforms

The regulatory treatment of fintech financing platforms[9] will be determined based on their business models. The following guideline will be followed for licensing of fintech financing platforms:

(a) **Banking Regulation** - a fintech platform whose business model involves deposit taking from the public will be subjected to existing banking regulation with added technology specific policy requirements, which includes the following:

- Bank of Botswana (Amendment) Act (CAP 55:01) as amended;
- Banking Act (2023);
- Banking Regulations (2025);
- Financial Intelligence Act (2022);
- Financial Intelligence Regulations (2022);
- Financial Intelligence (Implementation of UNSCR) Regulations (2022);
- Consumer Protection Act (CAP 42:07);
- Competition Act (2018);
- Data Protection Act (2024);
- National Financial Services Cyber Security Framework;
- Open Banking Policy;
- Application Programming Interface Guidelines;
- Artificial Intelligence/Machine Learning Policy;
- Cloud Computing Security Guidelines; and
- any other relevant legal instruments developed from time to time.

(b) **Securities Regulation** - a fintech platform whose business model issues and sells securities (e.g., to finance the purchase of loans), provides related investment advice or establishes secondary markets for the loans or investments it intermediates, will be

[9] Fintech platforms may accept money from investors on their balance sheet and lend out to borrowers or use to buy securities, while some fintech platforms may act exclusively as brokers between investors and those seeking funding. Some platforms that intermediate lending may use their own balance sheet to retain some of the credit risks while others may pass the entire credit risk on to investors.

subjected to licensing or registration requirements under the existing securities regulation with added technology specific policy requirements, which includes the following:

- Securities Act (Persons Operating a Securities Infrastructure Business) (2017);
- Securities (Institutions Licensing) Regulations (2017);
- Securities (Online Trading Services) Regulations (2020);
- Collective Investment Undertakings (CIUS) Act (2021);
- Financial Intelligence Act (2022);
- Financial Intelligence Regulations (2022);
- Financial Intelligence (Implementation of UNSCR) Regulations (2022);
- Consumer Protection Act (CAP 42:07);
- Competition Act (2018);
- Data Protection Act (2024);
- National Financial Services Cyber Security Framework;
- Open Banking Policy;
- Artificial Intelligence/Machine Learning Policy;
- Application Programming Interface Guidelines; and
- Cloud Computing Security Guidelines.

(c) **Payments Regulation** – a fintech platform whose business model provides payment services such as initiation of payments on behalf of a customer, operates payment accounts to channel funds between clients, or initiates payments on behalf of clients from clients' payment accounts held elsewhere shall be subjected to the following:

- National Payment System Law (Drafting Underway)
- Electronic Payment Services Regulations (2019);
- National Clearance and Settlement Systems (NCSS) Act (CAP 46:06);
- NCSS Regulations (2005);
- Financial Intelligence Act (2022);
- Financial Intelligence Regulations (2022);
- Financial Intelligence (Implementation of UNSCR) Regulations (2022);
- Consumer Protection Act (CAP 42:07);
- Competition Act (2018);
- Data Protection Act (2024);
- National Financial Services Cyber Security Framework;
- Open Banking Policy;
- Artificial Intelligence/Machine Learning Policy;
- Application Programming Interface Guidelines;
- Distributed Ledger Technology Guidelines;
- Cloud Computing Security Guidelines; and
- any other relevant legal instruments developed from time to time.

5.2.4. Fintech Balance Sheet Lending

Licensing requirements for fintech firms providing fintech balance sheet lending[10] services will be the same as for non-bank microlending financial institutions with added technology specific policy requirements. Legal and regulatory frameworks that follow will apply for fintech firms whose business models facilitate fintech balance sheet lending:

(a) NBFIRA Act (2023);
(b) Micro Lending Regulations (2012);
(c) Financial Intelligence Act (2022);
(d) Financial Intelligence Regulations (2022);
(e) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(f) Consumer Protection Act (CAP 42:07);
(g) Competition Act (2018);
(h) National Financial Services Cyber Security Framework;
(i) Open Banking Policy;
(j) Artificial Intelligence/Machine Learning Policy;
(k) Application Programming Interface Guidelines;
(l) Cloud Computing Security Guidelines; and
(m) any other relevant legal instruments developed from time to time.

More specifically, Fintech Balance Sheet Lending platforms will be assessed for compliance with the requirement to assume the risk and be directly liable for any losses as well as obtaining authorisation prior to operation.

5.2.5. Loan and Equity Crowdfunding

Regulatory requirements for fintech firms whose business models facilitate loan and equity crowdfunding[11] will be focussed on consumer and investor protection, anti-money laundering/combating the financing of terrorism and counter proliferation financing (AML/CFT/CPF), business continuity and operational resilience, transparency, risk management, governance, and capital requirements. The following will apply to fintech firms providing loan and equity crowdfunding services:

(a) Banking Act (2023);
(b) Banking Regulations (2025);
(c) Financial Intelligence Act (2022);
(d) Financial Intelligence Regulations (2022);
(e) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(f) Consumer Protection Act (CAP 42:07);
(g) Competition Act (2018);
(h) Data Protection Act (2024);
(i) National Financial Services Cyber Security Framework;
(j) Open Banking Policy;

[10] Credit activity facilitated by non-bank lenders that use their own balance sheet to provide credit to borrowers through electronic channels.
[11] There is currently no regulatory framework for regulating loan and equity crowdfunding service providers. A recommendation for formulation of a requisite policy instrument is detailed under Recommended Policy Responses.

(k) Artificial Intelligence/Machine Learning Policy;
(l) Application Programming Interface Guidelines;
(m) Cloud Computing Security Guidelines; and
(n) Any other relevant legal instruments developed from time to time.

More specifically, Loan and Equity Crowdfunding platforms will be assessed for:

(a) Transparency - disclosure of information on risks, the platform, and conflicts of interest;
(b) Know Your Customer (KYC) and AML/CFT/CPF - due diligence checks on borrowers and/or issuers to establish the identity of investors and borrowers/issuers;
(c) Safekeeping of clients' (investor) funds - mandated use of a licensed bank or trust account that is separated from own funds;
(d) Risk Management - internal procedures for conducting due diligence on potential fundraisers and borrowers, procedures for selecting projects and publishing related information, minimum standards for credit risk analysis;
(e) Thresholds and eligibility - caps on amounts per issue or loan, caps on amount an investor can invest, restrictions based on type of investor;
(f) Governance, fitness and proprietary - requirement to have a risk, compliance and internal audit function, sufficient professional qualifications of managers and directors;
(g) Risk retention - requirement to retain the credit risk;
(h) Business continuity – wind down plans and resolution procedures;
(i) Prudential requirements - minimum capital or the requirement to take out a professional liability insurance policy to cover loan amounts; and
(j) Authorisation prior to operation.

5.2.6. Robo-Advisory

Regulatory regimes for financial advice will focus on addressing technology risks to afford clients of both robo-advisors and traditional investment advisors the same quality of investment service. In that regard, robo-advisors will be subjected to the "same activity, same risk, same regulatory outcomes" principle under the incumbent financial services regulations with added technology specific policy requirements. The following will apply to robo-advisors:

(a) NBFIRA Act (2023);
(b) Securities Act (Persons Operating as Securities Infrastructure Business) (2017);
(c) Securities (Institutions Licensing) Regulations (2017);
(d) Collective Investment Undertakings (CIUS) Act (2021);
(e) Online Trading Services Regulations (2021);
(f) Financial Intelligence Act (2022);
(g) Financial Intelligence Regulations (2022);
(h) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(i) National Financial Services Cyber Security Framework;
(j) Open Banking Policy;
(k) Artificial Intelligence/Machine Learning Policy;
(l) Application Programming Interface Guidelines;
(m) Cloud Computing Security Guidelines;
(n) Consumer Protection Act (CAP 42:07);
(o) Competition Act (2018); and

(p) Any other relevant legal instruments developed from time to time.

Robo Advisory services shall be assessed for:

(a) Governance arrangements for ethical and appropriate use of algorithms;
(b) Provision of comprehensive personalised advice (as opposed to scaled general advice);
(c) Best interest duty on provision of suitable algorithm-based advice and collection of customer information; and
(d) Disclosures to clients.

5.2.7. Insurtech

InsurTech business models will be subjected to existing licensing regimes and regulatory requirements, which are considered sufficient to address features of emerging innovative InsurTech business models when coupled with the technology specific policies and risk assessment requirements detailed in Section 5.3. The following will apply to InsurTech business models:

(a) NBFIRA Act (2023);
(b) Insurance Industry Act (2014);
(c) Insurance Industry Regulations (2019);
(d) International Insurance Act;
(e) Financial Intelligence Act (2022);
(f) Financial Intelligence Regulations (2022);
(g) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(h) National Financial Services Cyber Security Framework;
(i) Open Banking Policy;
(j) Application Programming Interface Guidelines;
(k) Cloud Computing Security Guidelines;
(l) Artificial Intelligence/Machine Learning Policy;
(m) Consumer Protection Act (CAP 42:07);
(n) Competition Act (2018); and
(o) any other relevant legal instruments developed from time to time.

5.2.8. Virtual Assets Related Financial Services (Digital Tokens)

A digital token (crypto/virtual/digital asset) will be defined as a digital or electronic representation of value that may be transferred, stored, and traded electronically, and may be used as a means of payment or exchange, store of value or unit of account.

5.2.8.1. Virtual Assets

Virtual assets will encompass digital assets issued by the private sector that depend primarily on cryptography and distributed ledger or similar technology. This Framework differentiates between function based and asset backed virtual assets based on the following criteria:

(a) underlying economic function (payment tokens, security tokens, utility tokens); and
(b) underlying assets (where the virtual assets may be backed by a fiat currency, commodities (precious metal), real estate or securities.

Moreover, virtual assets activities carried out under each of the above virtual asset classes will be categorised as follows:

(a) Issuance activities (creation, issuance, distribution and redemption);
(b) Operation of a DLT infrastructure activities (validation and settlement of transactions with virtual assets); or
(c) Service provision activities (digital wallet, custody, payment, exchange, trading, lending, borrowing or risk management services).

The regulatory treatment of virtual assets services will, therefore, follow the basic principle of "same activity, same risks, same regulatory outcomes" wherein if the economic function and purpose of a virtual asset service are the same as a regulated activity, then the virtual asset service shall be subject to the same regulatory frameworks on AML/CFT/CPF, securities trading, banking, payments, fund management, or financial infrastructure regulation. Similarly, if an entity or intermediary is engaging in activities with virtual assets that are by nature similar to those performed by regulated financial services providers or intermediaries, then such activities will be subjected to the same financial regulation.

Tokenised Payment Services (Payment Service Providers)

The following will apply for the regulation of virtual assets services dealing in payment tokens or facilitating payment services:

(a) Virtual Assets Act (2025);
(b) Virtual Assets Regulations, 2022;
(c) National Payment System Law (Drafting underway)
(d) Financial Intelligence Act (2022);
(e) Financial Intelligence Regulations (2022);
(f) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(g) Consumer Protection Act (CAP 42:07);
(h) Competition Act (2018);
(i) Data Protection Act (2024);
(j) National Financial Services Cyber Security Framework;
(k) Open Banking Policy;
(l) Artificial Intelligence/Machine Learning Policy;
(m) Application Programming Interface Guidelines;
(n) Distributed Ledger Technology Guidelines;
(o) Cloud Computing Security Guidelines; and
(p) any other relevant legal instruments developed from time to time.

Tokenised Securities Services

The following will apply for the regulation of virtual assets services dealing in securities tokens:

(a) Virtual Assets Act (2025);
(b) Virtual Assets Regulations (2022);
(c) Securities Act, 2014 and Securities (Amendment) Act (2023);
(d) Securities Businesses Regulations (2017);
(e) Collective Investment Undertakings Act (2021);

(f) Financial Intelligence Act (2022);
(g) Financial Intelligence Regulations (2022);
(h) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(i) Consumer Protection Act (CAP 42:07);
(j) Competition Act (2018);
(k) Data Protection Act (2024);
(l) National Financial Services Cyber Security Framework;
(m) Open Banking Policy;
(n) Artificial Intelligence/Machine Learning Policy;
(o) Application Programming Interface Guidelines;
(p) Distributed Ledger Technology Guidelines;
(q) Cloud Computing Security Guidelines; and
(r) any other relevant legal instruments developed from time to time

Utilities Tokens

The following will apply for the regulation of virtual assets classified as utilities tokens:

(a) Virtual Assets Act (2025);
(b) Virtual Assets Regulations (2022);
(c) Collective Investment Undertakings Act (2021);
(d) Financial Intelligence Act (2022);
(e) Financial Intelligence Regulations (2022);
(f) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(g) Consumer Protection Act (CAP 42:07);
(h) Competition Act (2018);
(i) Data Protection Act (2024);
(j) National Financial Services Cyber Security Framework;
(k) Open Banking Policy;
(l) Artificial Intelligence/Machine Learning Policy;
(m) Application Programming Interface Guidelines;
(n) Distributed Ledger Technology Guidelines;
(o) Cloud Computing Security Guidelines; and
(p) any other relevant legal instruments developed from time to time.

Specific Virtual Assets Regulatory Requirements

Over and above subjection to specific legal and regulatory frameworks listed above, and irrespective of whether virtual assets are a means of payment, an investment instrument, store of value, associated with securities or commodities, the regulatory treatment of virtual assets will cover the following key regulatory requirements, which are centred around licensing, prudential supervision, AML/CFT/CPF supervision, and consumer protection:

(a) **Governance**: virtual asset issuers and service providers will be required to have in place and disclose a comprehensive Governance Framework. The Governance Framework should be proportionate to their risk, size, complexity, and systemic importance, and to the financial stability risk that may be posed by the activity or market in which the issuer or service provider is participating. The Governance Framework should provide for clear and direct lines of responsibility and accountability for the functions and activities conducted by the issuer;

(b) **Risk Management, Recovery, and Resolution Planning:** virtual asset issuers and service providers will be required to have an effective Risk Management Framework that comprehensively addresses all material risks associated with their activities. The Framework should be proportionate to their risk, size, complexity, and systemic importance, and to the financial stability risk that may be posed by the activity or market in which the virtual asset service provider is participating. To the extent necessary to achieve regulatory outcomes comparable to those of traditional financial services providers offering the same asset class/financial services, virtual asset issuers or service providers will be required to provide a Risk Management Framework that addresses the financial stability risk that may be posed by the activity or market in which they are participating;

(c) **Data Management:** virtual asset service providers will be required to have in place robust frameworks for collecting, storing, safeguarding, and timely and accurately reporting data, including relevant policies, procedures and infrastructures needed, in each case proportionate to their risk, size, complexity and systemic importance. Such data should be accessible as necessary and appropriate for fulfilment of regulatory, supervisory and oversight mandates;

(d) **Disclosures**: virtual asset service providers will be required to disclose to users and relevant stakeholders comprehensive, clear and transparent information regarding their operations, risk profiles and financial conditions, as well as the products they provide and activities they conduct;

(e) **Monitoring of interconnections within the crypto-asset ecosystem with the wider financial system:** virtual asset service providers will be required to disclose all relevant interconnections, both within the virtual asset ecosystem, as well as between the virtual asset ecosystem and the wider financial system, and institute a comprehensive Risk Management Framework to mitigate against financial stability risks that could arise from these interconnections and interdependencies. The Bank and NBFIRA shall monitor identified interconnectedness and address identified financial stability risks;

(f) **Multiple Functions**: virtual asset service providers that combine multiple functions and activities, will be required to separate functions and activities, as appropriate and will be subjected to regulation, supervision and oversight that comprehensively addresses the risks associated with individual functions/activities as well as the risks arising from the combination of functions. The Bank and NBFIRA will monitor and address financial stability risks arising from such provision or combination of multiple functions/activities.

(g) **AML/CFT/CPF and Reporting Requirements**: virtual asset service providers will be required to perform customer due diligence, transaction monitoring, suspicious transactions reporting, reporting of the number of holders of virtual assets and the volume of transactions, reporting of any technical or operational incident that could compromise the stability of the financial system;

(h) **Solvency and Liquidity**: virtual asset service providers will be subject to capital and liquidity requirements in the form of an insurance policy or an equivalent security mechanism (e.g. cash deposit, bank guarantee) to safeguard customer investments;

(i) **Exit Strategy** - virtual asset service providers will be required to have a comprehensively documented exit strategy;

5.2.8.2.Stablecoins and Global Stablecoins

A stablecoin will be defined as a virtual asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets. A Global Stablecoin (GCS) will be defined as a stablecoin with a potential reach and use across multiple jurisdictions and which could become systemically important in and across one or many jurisdictions, including as a means of payments and/or store of value.

The role of stablecoins and GCS arrangements as an alternative payment instrument and/or store of value could increase over time particularly when integrated into online platforms, peer-to-peer and micropayments as well as cross-border transactions, thereby raising regulatory arbitrage risks. The regulation of stablecoins would result in overlaps between mandates of the Bank and NBFIRA, with broader implications including investor protection, consumer protection, data and privacy, systemic risk, financial stability, monetary policy, and national security.

Stablecoins and Global Stablecoins Payment Services

The following will apply for the regulation of payment services dealing in Stablecoins and GSC arrangements:

(a) Virtual Assets Act (2025);
(b) Virtual Assets Regulations (2022);
(c) National Payment System Law (Drafting underway);
(d) Financial Intelligence Act (2022);
(e) Financial Intelligence Regulations (2022);
(f) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(g) Consumer Protection Act (CAP 42:07);
(h) Competition Act (2018);
(i) Data Protection Act (2024);
(j) National Financial Services Cyber Security Framework;
(k) Open Banking Policy;
(l) Artificial Intelligence/Machine Learning Policy;
(m) Application Programming Interface Guidelines;
(n) Distributed Ledger Technology Guidelines;
(o) Cloud Computing Security Guidelines; and
(p) any other relevant legal instruments developed from time to time.

Stablecoins and Global Stablecoins Investment Services

The following will apply for the regulation of investment services dealing in Stablecoins and GSC arrangements:

(a) Virtual Assets Act (2025);
(b) Virtual Assets Regulations (2022);

(c) Collective Investment Undertakings Act (2021);
(d) Financial Intelligence Act (2022);
(e) Financial Intelligence Regulations (2022);
(f) Financial Intelligence (Implementation of UNSCR) Regulations (2022);
(g) Consumer Protection Act (CAP 42:07);
(h) Competition Act (2018);
(i) Data Protection Act (2024);
(j) National Financial Services Cyber Security Framework;
(k) Open Banking Policy;
(l) Artificial Intelligence/Machine Learning Policy;
(m) Application Programming Interface Guidelines;
(n) Distributed Ledger Technology Guidelines;
(o) Cloud Computing Security Guidelines; and
(p) any other relevant legal instruments developed from time to time.

The regulatory treatment and assessment of Stablecoins and GSC arrangements, over and above function specific regulatory frameworks irrespective of whether GSCs are a means of payment or an investment instrument will be as follows:

(a) **Regulatory Powers**: NBFIRA and the Bank will exercise the necessary powers within existing legal and regulatory frameworks and adequate innovation facilitator resources, to comprehensively regulate, supervise and oversee Stablecoins and GSC arrangements and their associated functions and activities, and enforce relevant laws and regulations effectively. Applicable innovation facilitator resources may include Regulatory Sandboxes, Innovation Hubs, and Innovation Accelerators for pilot testing Stablecoins and GSC arrangements under regulator-controlled environments;

(b) **Governance Framework**: Stablecoins and GSC arrangements will be required to institute comprehensive Governance Frameworks with clear allocation of accountability for the functions and activities within the GSC arrangement;

(c) **Risk Management Framework**: Stablecoins and GSC arrangements will be required to institute effective Risk Management Frameworks with regard to reserve management, operational resilience, cyber security safeguards, as well as "fit and proper" requirements;

(d) **Solvency and Liquidity**: Stablecoin and GSC arrangements will be subject to capital and liquidity requirements;

(e) **Robust Data Management Systems**: Stablecoins and GSC arrangements will be required to demonstrate existence of robust systems for collecting, storing and safeguarding data;

(f) **Disaster Recovery and Resolution Planning**: Stablecoins and GSC arrangements will be required to demonstrate existence of appropriate recovery and resolution plans;

(g) **Disclosures**: Stablecoins and GSC arrangements will be required to provide comprehensive and transparent information to users and relevant stakeholders on their functioning including information on their stabilisation mechanism;

(h) **Legal Clarity on Redemption Rights and Stabilisation Mechanisms**: Stablecoins and GSC arrangements will be required to provide legal clarity to users on the nature and enforceability of any redemption rights and the process for redemption, where applicable;

(i) **AML/CFT/CPF Requirements**: Stablecoin and GSC arrangements will be required to perform customer due diligence, transaction monitoring, suspicious transactions reporting, reporting of the number of holders of stablecoins and the volume of transactions, reporting of any technical or operational incident that could compromise the stability of the financial system;

(j) **Proportionate Regulatory, Supervisory and Oversight Requirements**: regulatory, supervisory and oversight regimes for Stablecoins and GSC arrangements will be functional based (payments or investment etc) as detailed under applicable legal and regulatory frameworks and proportionate to the risks they pose to the financial system;

(k) **Cross-Border Regulatory Cooperation and Coordination**: NBFIRA and the Bank will cooperate and coordinate with each other, on both domestic and cross-border fintech matters, to foster efficient and effective communication, consultation, information sharing, and alignment of legal and regulatory frameworks in fulfilling their respective mandates to ensure comprehensive regulation, supervision, and oversight of digital payment tokens, Stablecoins and GSC arrangements across sectors and borders;

(l) **Exit Strategy** - Stablecoin and GSC arrangements will be required to have a comprehensively documented exit strategy;

(m) **Licensing Requirements**: Stablecoins and GSC arrangements will be assessed for compliance with all applicable regulatory requirements to attain compliance before commencing any operations and adapting to new regulatory requirements as necessary.

5.2.9. Designation of Payment Systems for Oversight

In line with the Principles for Financial Market Infrastructures (PFMIs), high risk fintech driven payment systems with systemic profiles will be designated as Systemically Important Payment Systems (SIPS). Criteria that will be used for designation of fintech driven systems as SIPS or Non-SIPS will include fintech driven systems that:

(a) are the sole payment system in Botswana;
(b) are the principal system in terms of the aggregate value of payments;
(c) mainly handle time-critical, high-value payments; and
(d) settle payments used to effect settlement in other systemically important Financial Market Infrastructures (FMIs).

Criteria that shall be considered in determining the need for or regulatory intensity for various types of fintech related FMIs will include the following:

(a) **Number and Value of Transactions Processed** - low transaction volumes and values will require low regulatory intensity while high transaction volumes and values will require high regulatory intensity;

(b) **Number and Type of Participants** – a low number of participants will require low regulatory intensity while a high number of participants will require high regulatory intensity;

(c) **Markets Served** – ow risk markets will require low regulatory intensity whereas high risk markets will require high regulatory intensity;

(d) **Market Share Controlled** – a low market share will require low regulatory intensity while a high market share will require high regulatory intensity;

(e) **Interconnectedness with other FMIs and other Financial Institutions** - minimal interconnectedness will require minimal regulatory intensity while a high degree of interconnectedness will require high regulatory intensity; and

(f) **Available Alternatives to using the FMI at Short Notice** - existence of alternatives will warrant low regulatory intensity whereas non-existence of alternatives will require a high degree of regulatory intensity.

Payment system infrastructure designation decisions will be informed by regulatory intensity and system risk profile as follows:

(a) **Highly Regulated** - SIPS that handle large-value and time-critical payments will be subject to high regulation and compliance requirements to applicable sector specific, national, and international standards;

(b) **Moderately Regulated** - critical service providers (CSPs) including technology platform providers, and messaging providers will be subject to regulatory oversight;

(c) **Less Regulated** - informal funds transfers[12] (IFT) will be subjected to less/minimal regulatory oversight.

The Botswana financial services regulatory authorities will designate emerging fintech driven payment system infrastructures and payment services providers based on their risk profiles and requisite regulatory intensity based on key features as SIPS or non-SIPS. Following identification and designation, fintech driven payment system infrastructures and payment services providers will be subjected to the relevant international standards, local and international legal frameworks, and any other regulatory requirements that supplement payment systems regulations and policies.

5.3. STEP 3: RISK ANALYSIS AND MANAGEMENT

The third step in the Fintech Analytical Assessment Framework is identification and assessment of any emerging fintech related risks that may not be effectively addressed by existing legal and regulatory frameworks. A comprehensive assessment of risks will be undertaken to ensure that fintech firms and fintech service providers' Risk Management Frameworks entail risk mitigation measures that adequately address all potential risks. Fintech related risks fall into seven (7) categories as follows:

[12] Refers to money transfers that occur in the absence of, or are parallel to, formal payment services channels.

(a) Virtual assets related risks;
(b) Funds protection risks;
(c) Financial integrity risks;
(d) Cyber and data security risks;
(e) Access to payment systems risks;
(f) Interoperability risks; and
(g) Consumer protections risks.

Table 1 presents a Fintech Activities Inherent Risk Rating Map based on each activity's inherent risks as informed by the inherent nature of the activity and underlying technologies.

	Approximate Risks						
Fintech Driven Services	Funds Protection	Financial Integrity	Cyber and Data Security	Access to PCS[13] Systems	Inter-operability	Consumer Protection	Virtual Assets Related Risks
Account Issuance Services	M	H	H/H	L	M	H	H
E-Money Issuance	H	H	H/M	M	L	H	H
Domestic Funds Transfers	H	H	H/M	H	L	H	H
Cross-Border Funds Transfers	H	H	H/M	H	L	H	H
Merchant Acquisition Services	H	L	H/M	M	M	M	H
Digital Payment Services	M	H	H/M	H	L	H	H
Fintech Platform Financing	H	H	H/H	M	M	H	H
Loan Crowdfunding Services	H	H	H/H	M	M	H	H
Equity Crowdfunding Services	H	H	H/H	M	M	H	H
Robo-Advisory Services	L	H	H/H	M	M	H	H
InsurTech Business Models	L	H	H/H	M	M	H	H
Digital Token Services (VAs, Stablecoins and GSCs)	H	H	H/H	H	M	H	H

NB: Approximate inherent risks based on generic operating models. H = High, M = Moderate, L = Low

Table 1 Fintech Activities Inherent Risk Rating Map
(Source: Adapted from IMF)

[13] Payment, Clearing and Settlement Systems

The Bank and NBFIRA shall comprehensively assess Risk Management Frameworks provided by fintech firms applying for licensing for provision of fintech driven financial services detailed in Table 1 above for adequacy of the requisite risk mitigation measures for each of the corresponding risks identified per fintech financial service/activity.

5.3.1. Virtual Assets Related Risks

Depending on their characteristics, virtual assets, banks, and by extension, non-bank financial services providers may potentially be exposed to risks emanating from virtual assets. In that regard, assessment of fintech service providers inclusive of VAs and VASPs for licensing and ongoing regulatory compliance as well as other financial services providers dealing with, directly or indirectly impacted by virtual assets shall entail a comprehensive assessment of their Risk Management Frameworks for demonstration of existence of adequate control measures for the following virtual assets related risks:

(a) **Liquidity Risk**: the risk that financial services providers that hold virtual assets may not be able to convert them into fiat currency at little or no loss of value in private markets, thereby exposing them to market liquidity risk. In that regard, fintech service providers and incumbent financial services providers will be assessed for liquidity risk that may be directly or indirectly linked to virtual assets;

(b) **Market Risk**: the risk that the high degree of volatility in the valuation and pricing of non-fiat currency backed virtual assets could expose fintech services and incumbent financial service providers to losses. Fintech service providers and incumbent financial services providers will, therefore, be assessed for market risk that may be directly or indirectly linked to virtual assets;

(c) **Credit and Counterparty Credit Risk**[14]: the risk that fintech service providers and incumbent financial services providers may be directly or indirectly subject to credit risk due to exposures to virtual assets. In that regard, fintech service providers and incumbent financial services providers will, therefore, be assessed for credit and counterparty credit risk that may be directly or indirectly linked to virtual assets;

(d) **Cyber and Operational Risks**: the risk that financial services with exposures to virtual assets, or financial services that may provide related services, could be subject to technological vulnerabilities and cyber-attacks. In that regard, fintech service providers and incumbent financial services providers will, therefore, be assessed for cyber and operational risks directly or indirectly linked to virtual assets;

(e) **Legal Risks**: the risk that uncertainties related to the legal status of virtual assets and their broader ecosystem could expose financial services to legal risks, potentially including consumer protection, misconduct related to ML/FT/PF, and cross-border legal and regulatory requirements. In that regard, fintech service providers and incumbent financial services providers will, therefore, be assessed for legal risk that may be directly or indirectly linked to virtual assets;

[14] Financial services lending to entities that invest in virtual assets or that form part of a virtual asset ecosystem may have difficulties adequately pricing the risk of the borrower defaulting on loans due to the lack of historical data on virtual assets. In addition, banks could potentially be exposed to non-financial risks as a result of their direct or indirect exposures to virtual assets and related services.

(f) **Reputational Risks**: the risk that financial services that promote or enable the use of virtual assets could face reputational risk in the event of any losses incurred by virtual asset holders, misconduct by any service provider involved in the virtual assets ecosystem, or broader vulnerabilities that emerge in the network. In that regard, fintech service providers and incumbent financial services providers will, therefore, be assessed for reputational risk that may be directly or indirectly linked to virtual assets;

(g) **Third-Party Risks**: the risk that financial services that rely on third parties to develop and/or support virtual asset related activities could potentially be exposed to the risk of disruption of operations and services provided by such counterparties. In that regard, fintech service providers and incumbent financial services providers will, therefore, be assessed for third party risks that may be directly or indirectly linked to virtual assets; and

(h) **Implementation Risks**: the risk that financial services providers' role within a virtual asset ecosystem may require internal changes to systems and controls, which could be subject to implementation risks. In that regard, fintech service providers and incumbent financial services providers will, therefore, be assessed for implementation risk that may be directly or indirectly linked to virtual assets or virtual assets service providers.

5.3.2. Funds Protection Risks

With regards eMoney issuance and other fintech activities involving holding of customer funds by service providers, the Botswana financial services regulatory authorities' assessment of fintech activities for licensing and ongoing regulatory compliance will entail ascertaining compliance with the following funds protection risk control measures to safeguard customer funds and bolster user confidence in using fintech driven services:

(a) initial and ongoing regulatory capital requirements;
(b) maintenance and management of a dedicated trust account;
(c) trust account management agreements with partner settlement banks; and
(d) daily reconciliation of trust accounts;

These control mechanisms intended to safeguard customer funds, require that funds held in the dedicated trust account must always be equivalent to the total amount of electronic money balance held by the issuer. Funds in transit, with respect to funds transfer and payment aggregation services, will also be subjected to the same safeguarding requirements as electronic money.

5.3.3. Financial Integrity Risks

Fintech services have a potential of being used for money-laundering and terrorist financing. Fintech services inclusive of VAs and VASPs that fall within the scope of a product, service, or activity that is covered by FATF standards on AML/CFT/CPF supervision will be subject to AML/CFT/CPF requirements and supervision commensurate with the nature, scale, and risks of their activities to maintain the integrity and stability of the national payment system.

AML/CFT/CPF requirements in line with the Financial Intelligence Act, 2022, the Financial Intelligence Regulations, 2022, and the Financial Intelligence (Implementation of UNSCR)

Regulations, 2022, will be applied to reporting entities regardless of whether transactions are in fiat currency or digital tokens.

5.3.4. Cyber and Data Security Risks

Disruptive innovation inclusive of fintech services inherently carries a high cyber risk and vulnerabilities stemming from the greater degree of interconnectedness and increased risks of contagion. Assessment of fintech activities per the Cyber Security Policy Framework for financial services will entail ascertaining adherence to all cyber-risk policy requirements as part of licensing, regulation, oversight and ongoing regulatory compliance. Assessment will focus on the risk of unauthorised access, information change, information destruction, funds extortion, and business interruption.

Assessment of fintech activities for cyber and data security risks will mandate fintech service providers to demonstrate existence of the following comprehensive cyber-risk policies as part of licensing, regulation, oversight and ongoing regulatory compliance:

(a) **Institutional Cyber Security Policy** – a comprehensive Cyber Security Policy that forms the foundation of the provision of fintech driven financial services;

(b) **Technology Risk Management Framework** - a sound and robust technology risk management framework that provides operational risk management practices for ensuring system resilience and safeguarding of customers from losses;

(c) **Cyber Security Tools and Authentication Mechanisms** – deployment of strong cyber security tools and authentication mechanisms to protect customer data, transactions and systems as well as gather the necessary cyber intelligence; and

(d) **Systems Security and Resilience Arrangements** – for strengthening system security, reliability, resilience, recoverability, and business continuity.

5.3.5. Access to Payments, Clearing and Securities Settlement Systems Risks

Access to payments, clearing, and securities settlement systems is currently restricted to financial institutions, which are required to meet high regulatory standards. Access criteria is set by system operators, in this case the Bank as the settlement provider, Bankers Association of Botswana as operator of the Botswana Automated Clearing House (BACH), and the Botswana Stock Exchange Limited as operator of the Central Securities Depository system through the Central Securities Depository Company of Botswana (CSDB).

Access considerations will be geared towards achievement and maintenance of public policy objectives of safety and efficiency. In that regard, risk assessment pertaining to eligibility for access to payments, clearing, and securities settlement systems will entail a comprehensive assessment of the adequacy of control for mitigating against the risk of financial system disruption. Risk-related participation assessment will ensure that participants meet operational, financial, and legal requirements per applicable legal and regulatory frameworks for payments, clearing, and securities settlement systems as well as licensing requirements detailed in this Framework. Assessment of risks relating to the following specific eligibility criteria will be undertaken:

(a) licensing status;
(b) transactions threshold;
(c) direct or indirect settlement as determined by the payment system operator; and
(d) settlement account, whose eligibility willl be the discretion of the Bank.

5.3.6. Interoperability Risks

The Bank and NBFIRA will mandate interoperability of all financial services infrastructure, innovations, and platforms through adherence to set API guidelines to prevent the risk of siloed ecosystems and market fragmentation.

The objective of mandating interoperability of financial services infrastructure and services is to enable the ease of integration of services, enhance confidence in the acceptance of fintech driven services; reinforce competition; facilitate commitment to open, free, and contestable markets where the playing field is level; promote innovation; provide consumer choice; and facilitate access to high-quality financial services. Assessment of interoperability risks will focus on:

(a) ability to integrate into existing financial services infrastructure;
(b) risk of closed loops; and
(c) compliance with the any Open Banking Policy and API Guidelines.

5.4. STEP 4: PROMOTING LEGAL CERTAINTY

Assessment of fintech activities for regulation and prudential supervision and oversight will entail ascertaining legal certainty to ensure that legal and regulatory frameworks comprehensively cover all emerging fintech activities and their associated risks. The current legal framework governing financial services as presented in Section 2 of this Framework will continually be adapted to emerging fintech developments. The Botswana financial services regulatory authorities will continually promote legal certainty through a transparent, comprehensive, and sound legal framework for financial services.

In response to the entry of fintech services into the financial services industry, the Botswana financial services regulatory authorities will adopt activity-based regulation for the regulatory treatment of fintech. This will be in alignment with the basic principle of "same activity, same risks, same regulation" or "same activity, same risks, same regulatory outcomes". This will involve adapting new technologies to existing laws and adjusting existing legal and regulatory frameworks to accommodate emerging technologies, hence promoting legal certainty for emerging fintech and achieving functional regulation.

The following key considerations will be applicable for promoting legal certainty of all emerging innovative fintech activities not comprehensively covered by existing legal and regulatory frameworks:

(a) **Adaptation of the Legal Framework to System Development** – regulatory frameworks and supervisory practices will be adapted for orderly development and stability of the financial system as well as facilitating the safe entry of new fintech products, activities, and intermediaries; sustaining trust and confidence in the financial system; and responding to risks. Legal reforms will be based on relevant "model laws" developed by international legal organisations;

(b) **Development of the Legal Framework Through Consultation** – the Botswana financial services regulatory authorities will consult all relevant stakeholders, NPS participants, and legislators for fundamental reform of the legal framework to facilitate an adequate and effective legal framework. An enabling legal framework will accommodate technological change, tailored to local national circumstances;

(c) **Legal Framework Transparency and Accessibility** – regulations, legislation, and system rules will be clearly drafted, making use of widely accepted standard form agreements. The laws and regulations will be publicly available and critical information contained therein easily accessible to all interested stakeholders;

(d) **Provision of a Legal Basis for Regulatory Functions** – the Botswana financial services regulatory authorities will derive oversight responsibilities and powers relating to emerging fintech services from explicit statutory instruments or from general agreements on overall functional mandates; and

(e) **Involvement of the Bank of Botswana in Payments and Clearing Systems** - where there are payments and settlement systems from other sources, e.g., virtual assets payments and settlement systems, the Bank will identify and monitor critical legal issues and implications for the National Payment System.

Figure 2 below depicts a schematic presentation of the process for ascertaining and promoting legal certainty of all emerging fintech services and activities.

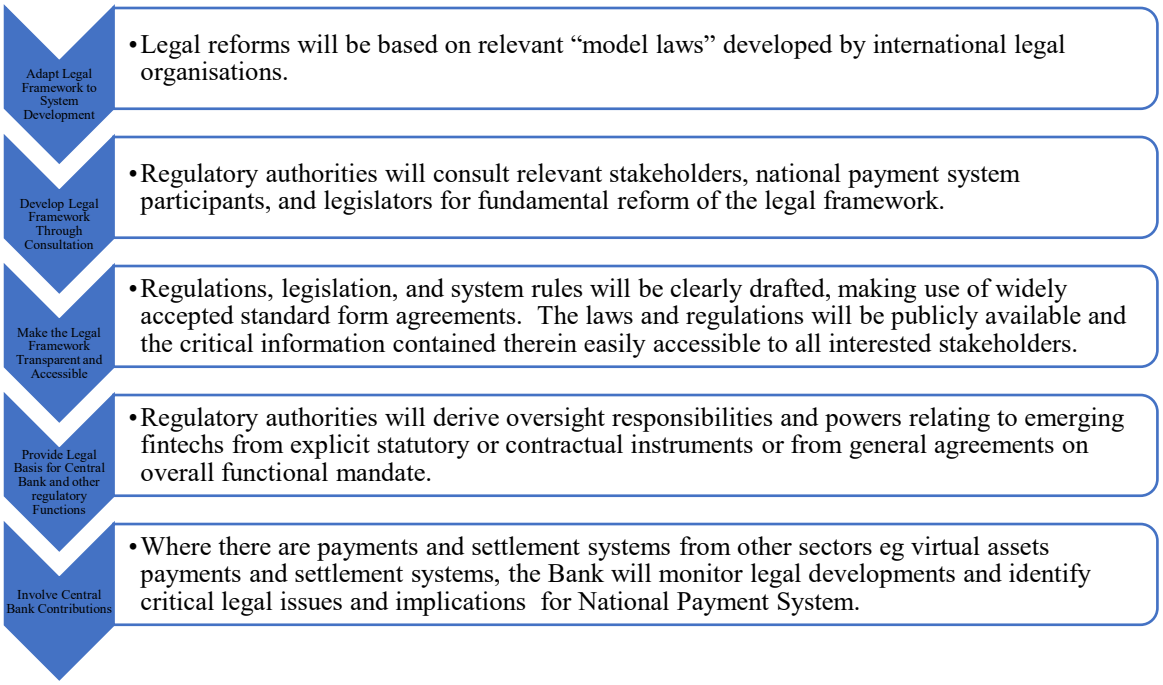


Figure 2 Key Considerations for Promoting Legal Certainty
(Adapted from the Committee on Payment and Settlement Systems)

Existing legal and regulatory frameworks will continually be reviewed to accommodate emerging fintech developments and shall be augmented by complementary directives that specifically address fintech related public policy concerns where there are regulatory gaps.

6 INNOVATION FACILITATORS

The financial services sector may establish, develop guidelines, and operate innovation facilitators to accelerate adoption of emerging innovative fintech services and facilitate safe and orderly market entry for emerging fintechs as follows:

6.1 Innovation Hubs

Sector specific innovation hubs may be established to provide support, advice, and guidance to both regulated and unregulated firms in navigating the regulatory landscape with a view to eliminate barriers to market entry, promote innovation, nurture ideas into innovative products and services with intellectual property (IP) protection, and promote technology development and technology transfers. Development of guidelines and policies for operation of sector specific innovation hubs in provision of regulatory guidance will be coordinated by regulatory authorities in collaboration with market stakeholders.

6.2 Regulatory Sandboxing

Regulatory authorities may establish sector specific regulatory sandboxes to serve as regulatory policy response tools geared towards facilitating testing of innovative solutions under supervision. Regulatory Sandboxing may be undertaken as part of the management of risk to the financial system, initiatives for fostering innovation, promotion of legal certainty for fintechs not covered by existing legal and regulatory frameworks, and elimination of barriers to market entry. Execution of the four step Fintech Analytical Assessment Framework culminates into regulatory sandboxing of emerging innovative fintech activities.

Having identified economic activities as fintech activities, assessed licensing and designation needs, identified emerging risks, and assessed adequacy of control measures as well as legal certainty, new fintech entities (startups) and emerging fintech activities will be subjected to regulatory sandboxing in line with set Regulatory Sandboxing Guidelines and related policies. The development of Regulatory Sandboxing Guidelines and policies will be coordinated by regulatory authorities in collaboration with market stakeholders.

6.3 Innovation Accelerators

Botswana financial services regulatory authorities may employ innovation accelerator initiatives such as Hackathons; wherein regulatory authorities may enter into strategic partnership arrangements with fintech providers for development of targeted and specific use cases that may involve funding support and/or endorsement by regulatory authorities and/or Government. Innovation accelerator initiatives will be undertaken in accordance with set guidelines for partnerships between the market and regulatory authorities and coordinated by regulatory authorities in alignment with provisions of the Competition Act (2018), Consumer Protection Act (CAP 42:07) and the Public Procurement Act (Cap 42:08).