GBBC GSMI 5.0

View the Full GSMI 5.0 DeFi Report Here

DeFi ACTIVITIES AND RISK ASSESSMENT APPROACH #1

While most jurisdictions lack clear regulatory frameworks for DeFi, active and informed risk management is possible. Common principles include:

- Consumer protection
- Market integrity, addressing market manipulation and fraud
- AML/CFT Measures
- KYC best practices
- Security and privacy
- Compliance

TRADITIONAL REGULATED ENTITIES

Entity	DeFi Functionality
Fund Managers & Asset Managers	• Trading & investing in tokens • Sophisticated financial solutions • Transparency on assets' performance
Brokerage Firms	• Trading • Improving liquidity • Considering becoming swap dealers
Market Makers & Liquidity Providers	• Liquidity provision
Central Banks	• Research and pilots on DeFi innovation to facilitate transactions in traditional financial system

Considerations & Obligations for Customers	Risks	Mitigation Measures
• Regulatory compliance & standards (e.g., custody requirements, separation of customer assets, market integrity) • Internal mandates • Duty of care to act in best interest of clients • Sanctions and AML compliance	• Monetary losses • Data breaches • Sanctions violations • AML and fraud • Predatory activities • Technical risks	• Insurance (including data) • Recovery mechanisms • Centralized KYC • Counterparty risk mitigation • Internal policies & procedures • Research, piloting, and testing

REGISTERED LEGAL ENTITIES OFFERING DIGITAL ASSET SERVICES

Entity	DeFi Functionality
Crypto Exchanges, Brokers, & Trading Platforms	• Trading • Staking services • Self custody wallets
Custodians & Wallets; Market Makers & Liquidity Providers	• Custody of tokens • Wallets may allow access to other DeFi services
Tokenization Platforms	• Tokenization of assets • Trading • DeFi reduces barriers to entry for adoption of tokenized assets
Stablecoin & Other Token Issuers	• Providing currency used for DeFi activities

Considerations & Obligations for Customers	Risks	Mitigation Measures
• Regulatory compliance • Registration and licensing • Best practices around product offerings (e.g., liquidity, market integrity, safeguarding funds, reserves/collateralization, transparency) • Risk mitigation programs • Secure and functioning backend, especially for data management • Access controls and permissions • Integration with DeFi platforms	• Counterparty risk upon leaving a DeFi platform • Monetary losses • Data breaches • Sanctions violations • AML and fraud • Technical risks	• Transparency and risk disclosures • Transaction monitoring and sanctions screening • Enhanced KYC • Insurance and recovery mechanisms • Counterparty analysis

View the Full GSMI 5.0 DeFi Report Here

DeFi ACTIVITIES AND RISK ASSESSMENT APPROACH #2

DeFi PROTOCOLS

Entity	DeFi Functionality
Layer 1 Protocols	• Smart contract layer on which to build DeFi applications • Sets of common rules enabling composable financial services and governance • Essential functions like security and settlement
DeFi Applications	• Wide range of alternative financial services
Decentralized Exchanges (DEXes)	• Exchange services
Bridges	• Interoperability solutions
Layer 2	• Scaling solutions, freeing up space at the L1 level for essential functions
Decentralized Autonomous Organizations (DAOs)	• Decentralized governance and decision making

Considerations & Obligations for Customers	Risks	Mitigation Measures
• Technical functionality • Best practices for execution (e.g., liquidity, exchange services, fair lending, records of transactions, verifications, offloading transaction execution) • Security and privacy • Truly decentralized functions and decision making	• Technical failures • Monetary losses • Data breaches • Consolidated control that is not fully and practically decentralized • Sanctions violations • AML and fraud • Cross-chain jurisdictional compliance violations between Layer 1s • Unequal representation of individual participants, leading to information asymmetries and abuses • Concentrations of power in voting and decision making • General partnership liability for violations of law	• Code and security audits • Best practices for programming • Full divestment of protocol control by founders and creators • RegTech solutions designed for DeFi • Insurance and recovery mechanisms • Mechanisms to overrule single voters • Mechanisms similar to traditional corporate accountability structures • Warn participants of general partnership liability exposure

KEY OPEN REGULATORY QUESTIONS FOR DeFi

- What constitutes a **true DeFi activity**?
- How do DeFi activities **fit into existing regulations,** and what are the **new regulatory expectations**?
- What is the **role of regulation when there are no intermediaries**?
  - Should any DeFi activities be treated as intermediaries, and who is responsible?
- What functionality should DeFi participants ensure to be **considered acceptable by regulators**?
- **Should DAOs be considered legal entities** and regulated as such?

KEY RECOMMENDATIONS FOR A DeFi PLAYBOOK

- **Definitions will help identify roles, responsibilities, and rules** for DeFi players
  - For instance, defining necessary elements of a DAO to merit that name
- **Establish standards and best practices for DeFi**, and what categories of activity they should apply to
- Consider measures for **governance, dispute resolution, AML/KYC, verifications, consumer protections, and other safeguards**
- **Define regulatory risks and mitigation measures**
- Consider an **iterative process** toward legislative and regulatory developments

DISCLAIMER:

- Additional categories include sandboxes and DeFi supporting services, covered in detail in the GSMI 5.0 DeFi report
- Individual users are not included in these categories because any potential harmful behavior on their part is already covered in multiple existing laws (e.g., fraud, market manipulation, hacks, etc.)
- The tables included in this document are summarized versions, please access the GSMI 5.0 DeFi Report for detailed information

Prepared 26 March 2025