

October 19, 2023

Mr. Martin Moloney
Secretary General
International Organization of Securities Commissions
C/ Oquendo 12,
28006 Madrid
SPAIN

By email: deficonsultation@iosco.org

Dear Sir,

Public Comment on IOSCO's Consultation Report on Policy Recommendations for Decentralized Finance (DeFi)

The Institute of International Finance (**IIF**) welcomes the opportunity to respond to the International Organization of Securities Commissions' (**IOSCO's**) [consultation report](#) containing proposed Policy Recommendations (**Recommendations**) for DeFi, released in September 2023.

We commend IOSCO for tackling these important issues in a consultative way. We also welcome IOSCO's close engagement with other international standard-setters engaged in efforts around these topics including those of the Financial Stability Board (**FSB**).

The IIF notes the abbreviated timeframe for responding to this consultation, and also duly notes that IOSCO has highlighted that these recommendations are complementary to those of the prior consultative report on crypto and digital asset markets. The IIF would suggest a **subsequent period** of public consultation would be prudent to consider IOSCO's full set of proposed recommendations to understand and address the implications of their combination.

The IIF notes the challenging nature of this consultation lies in there being a **continuum along which decentralization may exist**, and the interactions between centralized entities with more decentralized entities or processes require consideration. At present, the effect of the recommendations may be to create a binary decision, where an organization is either considered centralized or decentralized. This may lead to unintended consequences that may follow from differences in interpretation and/or implementation across jurisdictions, or from being subject to potentially different rules (e.g. that are entity-based rather than activity-based). This may make it more challenging for regulated entities to innovate and interact with developers or permissionless networks.

It is currently difficult to interpret the scope of what the IOSCO recommendations are intended to capture. A **clearer definition** of DeFi is required. At present, the recommendations have the potential to cast too broad a regulatory net, potentially bringing things within the regulatory perimeter that should not be captured. DeFi regulation should not bring asset classes or activities that are outside of the scope of financial market regulation into the scope of that regulation merely because of the use of decentralized ledger technology (**DLT**) or other decentralized aspects.¹

¹ The adoption of a DLT- or blockchain-based books and records system by a financial institution to record its deposit and custody balances, together with the provision of tokens acting as a reporting token or a tokenized receipt or method of instruction to an FI to issue a confirmation of a transaction recorded on the FI's book and records, should be scoped out. See response to Question 2 in Annex 1.

At time of writing, total value locked in DeFi protocols was around \$48 billion, less than 5% of the \$1.06 trillion total market capitalization of crypto-assets.² We note that the European Union has excluded fully decentralized financial services from the scope of MiCA, and the European Commission is not due to report finally on this topic until 2027, with an interim report due by mid-2025.³ The U.S. Congress has not passed specific legislation on crypto-assets, stablecoins or DeFi, which may be some years off, though regulators of course have existing mandates which they may seek to enforce against DeFi protocols or decentralized autonomous organizations (**DAOs**). Consequently, recommendations at this time should remain appropriately **high-level and flexible** to accommodate what is likely to be an evolving policy and legal landscape for some time across jurisdictions.

The IIF agrees with the principle of “**same risk, same regulatory outcome**” and would encourage IOSCO and its member regulators to apply it by requiring DeFi organizations to achieve the same outcomes intended by existing regulations, but not necessarily via the methods currently used to comply with existing regulations. It is advisable not to be overly prescriptive and allow organizations the flexibility to design compliance and disclosure programs that best (or better) fit the business model and technology used, tailored to adequately and appropriately reflect unique associated risks, as long as they achieve equal or better outcomes. IOSCO members should be encouraged to allow DeFi operations to explore highly automated or novel methods of delivering the same regulatory outcomes, consistent with the principles of safety and soundness expected of regulated financial institutions.

While recommendations for DeFi markets should not be more prescriptive or restrictive than those for other markets, proportionate to the risks they present, accountability must exist in the industry.

- The mapping exercise conducted by IOSCO matches DeFi activities with existing financial services counterparts to highlight similar risks posed. The combination of activities permitted within DeFi might also be appropriately considered as standalone products as the effects and risks of the **combination of activities** need to be accounted for, over and above the risks posed in traditional finance.
- **Conflicts of interest** require attention. By design, many or even most participants in a DeFi protocol have an “interest” in the protocol by virtue of staking. Accounting for all interests within a protocol may be an impossible threshold for many protocols to meet in their current form. The implications of this should be evaluated, as well as the most appropriate **disclosure** methods appropriate for retail and institutional users.
- At present, DeFi lacks sufficient accountability for **sanctions compliance**. One example is that gas fees could be paid to unknown actors that may be sanctioned entities. However, blockchain analytics and technological solutions such as verifiable credentials are under development to achieve accountability and require time to mature through iterative innovation, as well as institutional adoption of DeFi protocols via permissioned, public systems such as those envisaged in Project Guardian. Regulatory approaches today should ideally aim to ensure accountability and market integrity while simultaneously supporting the ability of such innovations to be developed tomorrow for the long-term betterment of the industry.

Some policy issues and recommendations related to DeFi that are addressed in a November 2022 IIF [staff paper](#) on DeFi, that are not covered in the IOSCO recommendations, may include the following:

1. A nuanced **decentralization spectrum** between centralized and decentralized models may emerge, rather than a binary ecosystem. This perspective argues for an integrated series of recommendations on crypto-assets, stablecoins and DeFi, with the DeFi regime ideally less prescriptive and more a set of lenses on the crypto

² DeFi Llama (excluding Double Count and Liquid Staking); coinmarketcap.com, as of October 10, 2023.

³ Article 140(2)(t) of Regulation (EU) 2023/1114 of the European Parliament and of the Council (**MiCA**).

- recommendations.⁴
2. IOSCO recommendations do not address the role of best practices or **technical standardization**, and should further focus on best practices around governance, cybersecurity, and code auditing as a key enabler of DeFi and to help the private sector build safe and efficient networks, noting that IOSCO members do not regulate developers, but the firms that engage them or use their protocols.⁵
 3. Anti-money laundering/combating the financing of terrorism (AML/CFT) and sanctions screening challenges posed by **pseudonymity** may necessitate engineered solutions like tokenized verifiable credentials and oracles, or permissioned, public systems. Recognition in the Recommendations of these issues would be helpful.⁶
 4. The IOSCO recommendations do not address the potential for **legal enablers of DeFi** around legal recognition of electronic transactions, transfer of and security over digital assets, and smart contract enforceability, and could usefully signpost efforts in that regard.
 5. Some DeFi protocols exist to manage payments and there is therefore a regulatory tie-in to **payments interoperability** and regulation that should be explored by the appropriate authority(s).
 6. We note IOSCO's use of the phrase "regardless of the technology that may be used to deliver financial products and services". We understand this phrase to be synonymous with "**technology neutrality**", and to be consistent with the principle of "same risk, same regulatory outcome."

Lastly, as we have done in relation to IOSCO's crypto-assets recommendations, we would urge the importance of an approach to regulation that recognizes the **dynamic nature** of the innovations underway and supports a framework designed to evolve in line with their responsible evolution.


We provide in **Annex 1** answers to the consultation questions, and in **Annex 2** additional comments on the wording of the Recommendations.

The IIF and its members stand ready to engage in additional discussions and consultations on these topics, or to clarify any aspect of our submission.

Yours sincerely,



Jessica Renier
Managing Director, Digital Finance



Andres Portilla
Managing Director, Regulatory Affairs

⁴ Further, the instance of 'quasi-decentralized' applications where whitelisting may be enforced through another entity despite the platform itself being public and permissionless is an important distinction. See Question 1 in Annex 1.

⁵ It would be appropriate for regulated participants of DeFi transactions to adhere to such technical standardization. It would not be appropriate for these standards to apply to developers of these protocols. See Question 7 in Annex 1.

⁶ For example, decentralized protocols exist that currently allow for transactions to take place without KYC/CDD. The enforcement of sanctions around Tornado Cash may provide guidance here, where blockchain analysis is conducted to determine origin/destination of funds deposited/withdrawn via digital asset 'on-off ramps' (exchanges, OTC, etc.).

Annex 1 – IIF responses to the consultation questions

Consultation question(s)	IIF response
<p>1. Do you agree with the Recommendations and guidance in this Report? Are there others that should be included?</p>	<p>The IIF agrees with the principle of “same risk, same regulatory outcome” and would encourage IOSCO and its member regulators to apply it by requiring DeFi organizations to achieve the same outcomes intended by existing regulations, but not necessarily via the methods currently used to comply with existing regulations. It is advisable not to be overly prescriptive and allow organizations the flexibility to design compliance and disclosure programs that best (or better) fit the business model and technology used, tailored to adequately and appropriately reflect unique associated risks, as long as they achieve equal or better outcomes. IOSCO members should be encouraged to allow DeFi operations to explore highly automated or novel methods of delivering the same regulatory outcomes, consistent with the principles of safety and soundness expected of regulated financial institutions.</p> <p>The IIF notes the challenging nature of this consultation lies in there being a continuum along which decentralization may exist, and the interactions between centralized entities with more decentralized entities or processes require consideration. At present, the effect of the recommendations may be to create a binary decision, where an organization is either considered centralized or decentralized. This may lead to unintended consequences that may follow from differences in interpretation and/or implementation across jurisdictions, or from being subject to potentially different rules (e.g. that are entity-based rather than activity-based). This may make it more challenging for regulated entities to innovate and interact with developers or permissionless networks.</p> <p>We provide detailed comments on the recommendations and accompanying guidance in Annex 2. What follows is subject to those comments:</p> <ol style="list-style-type: none"> 1. the mapping exercise conducted by IOSCO matches DeFi activities with existing financial services counterparts to highlight similar risks posed. The combination of activities permitted within DeFi

Consultation question(s)	IIF response
	<p>might also be appropriately considered as standalone products as the effects and risks of the combination of activities need to be accounted for, over and above the risks posed in traditional finance;</p> <ol style="list-style-type: none"> 2. the desirability of tailored regulation that adequately and appropriately reflects associated risks, implying also the need to avoid more prescriptive or restrictive requirements than for other markets, or the scoping in of activities purely because of the use of DeFi protocols; 3. the spectrum of decentralization raises a case for an integrated series of recommendations on crypto-assets, stablecoins and DeFi, with the latter more a set of lenses than prescriptive recommendations; 4. on timing, there is a case for additional steps to appropriately integrate this set of recommendations with the prior recommendations on crypto and digital asset markets; 5. the final report could usefully signpost the importance of technical standardization around code auditing and cybersecurity, and of legal enablers such as recognition of e-signatures and digital asset transfer and security; and 6. the challenge of pseudonymity and the possible role of tokenized verifiable credentials and oracles in AML/CFT and sanctions screening compliance should be acknowledged. <p>The discussion of cross-border enforcement (Rec. 8) and analysis for like services (Rec. 1) imply consistency in the structures of DeFi and permissible activities, but risk is not treated the same in all jurisdictions.</p> <p>Separately, some DeFi protocols exist to manage payments and there is therefore a regulatory tie-in to payments interoperability and regulations that should be explored by the appropriate authority(s).</p> <p>Further comments on the decentralization spectrum</p>

Consultation question(s)	IIF response
	<p>Particularly in the instance of ‘quasi-decentralized’ applications where whitelisting may be enforced through another entity despite the platform itself being public and permissionless, the whitelisting entity may not have control over the underlying application for which they are permitting access to, but performs a governance function around KYC. Without considering this spectrum, regulators risk stifling innovation and limiting the ‘out-of-the-box’ thinking that may result from DLT technology as an innovative financial platform. See also our comments on Rec. 2 and 6 regarding identifying responsible persons/entities.</p> <p>Further comments on materiality and timing</p> <p>It is important that new regulatory approaches are developed; in doing so, we encourage IOSCO to take into account that there is currently less than \$50 billion total value locked in the DeFi space, representing less than 5% of the overall crypto-asset market.⁷ Furthermore, when evaluating DeFi risks, it is important to note that, to date, interlinkages between DeFi, TradFi and the real economy are limited.⁸ Additionally, DeFi applications typically rely on intermediaries in the centralized crypto-asset market (exchanges, bridges, money service businesses) to on/off-ramp to fiat, providing a regulated touch point that can be addressed to mitigate risks in the value chain.⁹</p> <p>The EU has excluded fully decentralized financial services from the scope of MiCA. Instead, the European Commission has been charged with monitoring the DeFi market, and will report finally in 2027, and on an interim basis by mid-2025.</p> <p>While investor protection and financial stability aspects cannot be ignored, in our judgement IOSCO should ensure that its recommendations remain</p>

⁷ See footnote 2 for sources.

⁸ FSB (2023a), [The Financial Stability Risks of Decentralised Finance](#), p. 2; OECD (2022), [Why Decentralised Finance \(DeFi\) Matters and the Policy Implications](#), p. 53.

⁹ C.f. OECD, *op. cit.*, p. 54

Consultation question(s)	IIF response
	appropriately high-level, flexible, and tailored to accommodate what is likely to be an evolving policy and legal landscape for some time.
<p>2. Do you agree with the description of DeFi products, services, arrangements, and activities described in this Report? If not, please provide details.</p> <p>Are there others that have not been described? If so, please provide details.</p>	<p>It is currently difficult to interpret the scope of what the IOSCO recommendations are intended to capture. A clearer definition of DeFi is required. At present, the recommendations have the potential to cast too broad a regulatory net, potentially bringing things within the regulatory perimeter that should not be captured. The focus should be on entities that use DeFi arrangements to provide financial services, and potentially their responsible persons, rather than on technology or considerably indirect relationships that would be considered a stretch by way of applicability of the regulatory perimeter. DeFi regulation should not bring asset classes or activities that are outside of the scope of financial market regulation into the scope of that regulation merely because of the use of DLT or other decentralized aspects.</p> <p>The mapping exercise conducted by IOSCO matches DeFi activities with existing financial services counterparts to highlight similar risks posed. The combination of activities permitted within DeFi might also be appropriately considered as standalone products as the effects and risks of the combination of activities need to be accounted for, over and above the risks posed in traditional finance.</p> <p>Institutional DeFi, which takes many of the technologies of DeFi into a regulated and compliant setting subject to full customer due diligence (CDD), enabled by either whitelisted liquidity pools or zero-knowledge proofs, as discussed in the IIF’s November 2022 staff paper,¹⁰ may be a business model worth describing in more detail. Tokenized real assets could broaden access and stabilize prices.</p>

¹⁰ IIF (2022a), [Decentralized Finance: Use Cases, Challenges and Opportunities](#), pp 26-27

Consultation question(s)	IIF response
	<p>Some DeFi protocols exist to manage payments and there is therefore a regulatory tie-in to payments interoperability and regulations that should be explored by the appropriate authority(s).</p> <p>DeFi regulation should not prevent regulated financial institutions from exploring, developing, and using internal, private, permissioned blockchain or a DLT-based books and records system. As stated in our July 31 submission¹¹ to IOSCO on crypto and digital asset markets, the adoption of a DLT- or blockchain-based books and records system by a financial institution to record its deposit and custody balances should not change a traditional security, cash, or other asset into a “crypto-asset” or a “digital asset.” Such services, together with the provision of a reporting token or a tokenized receipt that an FI issues as confirmation of a transaction recorded on the FI’s books and records, should similarly be scoped outside of DeFi regulation. Such activities pose no additional risk beyond that already posed by book entries in existing, (non-DLT) electronic books and records systems used today, which is already covered by existing regulatory supervision and oversight.</p> <p>Similarly, a regulated financial institution that provides a service through which traditional securities or cash may be traded for another or settles such transaction utilizing a blockchain or DLT-based internal books and records system should not be considered a Decentralized Exchange.</p> <p>Finally, a reporting token or a tokenized receipt that a financial institution issues as confirmation of a transaction recorded on the financial institution’s books and records should also not be considered a crypto-asset or digital asset for the purpose of IOSCO’s Recommendations.</p>
<p>3. Do you agree with the Report’s assessment of governance mechanisms and how they operate in DeFi? If not, please provide details.</p>	<p>The governance assessment seems fair. The tension between distributed governance and concentration of power merits ongoing attention.</p>

¹¹ IF (2023b), [IIF submission to IOSCO on policy recommendations for crypto and digital asset markets](#)

Consultation question(s)	IIF response
	<p>It is worth noting that many DeFi systems display a considerable amount of economic, governance, or technical concentration and centralization. That said, a DeFi protocol may be associated with a foundation or DAO (incorporated or not), the governance token holders of which may seem a natural focus for supervision. However, we would caution that many or most token-holders in a DAO may not have sufficient interest to count as decision-makers. Simply having the status of being a token-holder is not sufficient. See further detail here on Recommendation 2 in Annex 2.</p> <p>If regulators choose to assess entities based on a level of decentralization, they should develop objective regulatory measures to assess the level of decentralization of a smart contract protocol. Such frameworks, for example, could take several indicators into account:</p> <ul style="list-style-type: none"> • the public availability of the protocol’s code or governance mechanisms; • the size of the total value locked or staked in a protocol; • the ability of persons or groups to significantly alter the core functionality of the protocol’s code; or • the ability of individuals to execute transactions without third-party approval. <p>Ultimately, decentralization is a spectrum, and where questions of governance remain, regulators should focus on identifying mechanisms to achieve consistent regulatory outcomes across that spectrum.</p> <p><u>Please refer also to our comments on Recommendation 2 (Identify responsible persons) in Annex 2.</u></p>
<p>4. Do you agree with the risks and issues around DeFi protocols identified in this Report? If not, please provide details. Are there others that have not been described? If so, please provide details. How can market participants help address these risks and/or issues, including through the use of technology? How</p>	<p>Conflicts of interest require particular attention in DeFi. These should be dealt with at the entity/responsible person level in providing financial services, rather than at the technology level. By design, many or even most participants in a DeFi protocol have an “interest” in the protocol by virtue of staking. Accounting for all interests within a protocol may be an impossible or highly impracticable threshold for many protocols to meet in</p>

Consultation question(s)	IIF response
<p>would you suggest IOSCO members address these risks and/or issues?</p>	<p>their current form. The implications of this should be evaluated, as well as the most appropriate disclosure methods for retail and institutional users.</p> <p>Overall, the risk discussion is fairly comprehensive. Adding a discussion of code vulnerabilities and composability risks and how to address them could strengthen it.¹² Stakeholders should collaborate to develop standards around selected risk management and governance topics such as cybersecurity risk or code audits. Standards and supervision that maintain accountability without stifling innovation may help address risks.</p> <p>AML/CFT and sanctions screening challenges posed by pseudonymity may necessitate engineered solutions like tokenized verifiable credentials and oracles, as well as institutional adoption of DeFi protocols via permissioned, public systems.¹³ Fostering the functioning of trusted digital identity solutions could mitigate know-your-customer (KYC) / anonymity challenges for DeFi arrangements and enable scalable access. Some recognition in the IOSCO Recommendations of the issues of AML/CFT or sanctions screening compliance, and/or of verifiable credentials as a means of compliance, would be helpful.</p> <p>The IOSCO recommendations do not address the potential for legal enablers of DeFi around legal recognition of electronic transactions, of transfer of and security over digital assets, and smart contract enforceability, and could usefully signpost efforts in that regard.</p> <p>Please also see our comments on recommendations 4 and 5 in Annex 2.</p>

¹² ‘Beyond technical standards that are tailored to each DeFi protocol or application, there may also be a role for technical standards to address **code security**, a key vulnerability around DeFi. Such technical standards could continue to be developed by individual protocols, or could be taken forward by standardization bodies such as the International Organization for Standardization (ISO), National Institute of Standards and Technology, or similar bodies. Another possible subject for standardization is the field of **code audits**, given a lack of audit’s role in code exploits. While at present many firms, including big DeFi firms such as Consensys, offer code auditing as a human- or AI-powered service, the field of DeFi code auditing and what is required is yet to be standardized. As TradFi seeks to do more business with DeFi and with DeFi tools, pressure can be expected to increase to ensure that “institutional DeFi” has its code base audited to a certain standard, and in line with standards that have been laid down independently of the particular project in question.’ – IIF (2022a), *op. cit.*, p. 41.

¹³ See IIF (2022a), *op. cit.*, p. 35.

Consultation question(s)	IIF response
<p>5. Do you agree with the description of data gaps and challenges in the Report? If not, please provide details. Are there others that have not been described? If so, please provide details. How can market participants address these data gaps and challenges, including through the use of technology? How would you suggest IOSCO members address data gaps and challenges?</p>	<p>The data challenges seem well described. Lack of data sharing across borders and between regulators are issues. The IIF has persistently advocated for the free flow of data with trust and gateways to enable sharing of supervisory data, among other categories of data.¹⁴ A recent IIF study focused on the impacts of data localization measures on AML/CFT compliance and advanced regtech solutions,¹⁵ and we continue to advocate for standardized information sharing “gateways” to address information barriers, for example in the context of cross-border payments,¹⁶ a position noted in the FSB’s recent stocktake on data frameworks.¹⁷</p> <p>Stakeholders collaborating to enable appropriate data access and analytics while protecting privacy could help. Regulators coordinating data collection and sharing could also assist.</p>
<p>6. Do you agree with the application of IOSCO Standards to DeFi activities contained in this Report? Are there other examples of how IOSCO Standards can apply?</p>	<p>The IIF agrees with the principle of “same risk, same regulatory outcome” and would encourage IOSCO and its member regulators to apply it by requiring DeFi organizations to achieve the same outcomes intended by existing regulations, but not necessarily via the methods currently used to comply with existing regulations.</p> <p>It is currently difficult to interpret the scope of what the IOSCO recommendations are intended to capture. A clearer definition of DeFi is required. At present, the recommendations have the potential to cast too broad a regulatory net, potentially bringing things within the regulatory perimeter that should not be captured. DeFi regulation should not bring asset classes or activities that are outside of the scope of financial market regulation into the scope of that regulation merely because of the use of DLT or other decentralized aspects.</p>

¹⁴ See IIF (2022b), [Submission to FSB on data frameworks affecting cross-border payments](#), in which G2G data sharing was called out as one suitable area for standardized gateways to be developed (at p. 5).

¹⁵ IIF (2023a), [Data Policy Impacts – AML and Regtech Solutions](#).

¹⁶ See IIF (2022b), *op. cit.*, p. 5.

¹⁷ FSB (2023b), [Stocktake of International Data Standards Relevant to Cross-border Payments](#), at p. 19.

Consultation question(s)	IIF response
	<p>Additionally, a clear articulation of the scope of IOSCO crypto-asset recommendations (with those applying to DeFi) will be important, particularly for those issuing decentralized stablecoins or other potentially systemically important instruments.</p> <p>The mapping exercise matches DeFi activities with existing financial services counterparts to highlight similar risks posed. The combination of activities permitted within DeFi should also be considered as standalone products, as the effects and risks of combinations of activities need to be accounted for over and above the risks posed in traditional finance.</p>
<p>7. Is there any additional guidance that you would find relevant to help IOSCO members comply with these Recommendations? If so, please provide details.</p>	<p>While the IOSCO Recommendations should be appropriately high-level at this time, recognizing yet-to-evolve approaches across a range of jurisdictions, IOSCO members should be encouraged to avoid interpreting or propagating regulations targeted at specific technologies, rather than the activities being conducted and the financial services being provided. This is consistent with regulatory approaches across the financial industry and with the principle of technology neutrality.</p> <p>Guidance on the applicability of standards to emerging models like DAOs could be useful. Promoting interoperability of rules across jurisdictions would support global consistency.</p> <p>Some DeFi protocols exist to manage payments and there is therefore a regulatory tie-in to payments interoperability and regulation that should be explored by the appropriate authority(s).</p> <p>As stated in the cover letter:</p> <ul style="list-style-type: none"> • IOSCO recommendations do not address the role of technical standardization, and should further focus on best practices around governance, cybersecurity, and code auditing as a key enabler of DeFi and to help the private sector build safe and efficient networks, noting that IOSCO members do not regulate developers, but the firms that engage them or use their

Consultation question(s)	IIF response
	<p>protocols.</p> <ul style="list-style-type: none"> • Anti-money laundering/combating the financing of terrorism (AML/CFT) and sanctions screening challenges posed by pseudonymity may necessitate engineered solutions like tokenized verifiable credentials and oracles, or permissioned, public systems. Recognition in the Recommendations of these issues would be helpful. • The IOSCO recommendations do not address the potential for legal enablers of DeFi around legal recognition of electronic transactions, of transfer of and security over digital assets, and smart contract enforceability, and could usefully signpost efforts in that regard. • Some DeFi protocols exist to manage payments and there is therefore a regulatory tie-in to payments interoperability and regulation, that should be explored by the appropriate authority(s). <p>Further comments on technical standardization</p> <p>It would be appropriate for regulated participants of DeFi transactions to adhere to such technical standardization around cybersecurity and code auditing similar to how publicly listed companies undergo audits of technology. This would broadly fit into existing technology risk and control, and operational resilience frameworks. At this time, it would not be appropriate for these standards to apply to developers of these protocols in part due to the lack of precedence around these standards enforced on open-source projects in the past but also due to the inherent difficulty in enforcement as there is no governance structure in place for the deployment of DeFi applications onto public permissionless chains (they can be deployed pseudonymously by any actor).</p>

Consultation question(s)	IIF response
	<p>Please see also Annex 2, which contains further comments on the Recommendations, and also on the accompanying guidance.</p>
<p>8. Given the importance of the application of IOSCO Standards to DeFi activities, are there technological innovations that allow regulators to support innovation in DeFi/blockchain technologies while at the same time addressing investor protection and market integrity risks? If so, please provide details.</p>	<p>One of the most helpful things IOSCO can do to provide consumer protection is to provide clarity on definitions, which will subsequently help to create clear standards and bring relevant activity within the regulatory perimeter, while at the same time incentivizing investment in novel compliance methods.</p> <p>Beyond that, technological innovations that can be facilitated in sandbox regimes and compliance accelerators could support early innovation in a safe environment. So-called “embedded supervision” enabled by technology could assist.¹⁸ Principles-based regulation focused on outcomes over identical rules would aid innovation.</p> <p>DeFi currently lacks sufficient accountability for sanctions compliance. One example is that gas fees could be paid to unknown (because pseudonymous) actors that may be sanctioned entities. However, blockchain analytics and technological solutions are under development to achieve accountability such as verifiable credentials and oracles,¹⁹ and require time to mature through iterative innovation, as well as institutional adoption of DeFi protocols via permissioned, public systems such as those envisaged in Project Guardian.</p> <p>Regulatory approaches today should ideally aim to ensure accountability while simultaneously supporting the ability of such innovations to be developed for the long-term betterment of the industry.</p>

¹⁸ Auer, R. (2022), [Embedded supervision: how to build regulation into decentralised finance](#), BIS Working Papers No 811

¹⁹ We note the existence of commercial “oracles” that are designed to indicate if particular blockchain addresses are the subject of sanctions, but which may not, as of yet, be able to reliably connect sanctioned but pseudonymous individuals to a given wallet address.

Consultation question(s)	IIF response
<p>9. Are there particular methods or mechanisms that regulators can use in evaluating DeFi products, services, arrangements, and activities, and other persons and entities involved with DeFi? If yes, please explain.</p>	<p>Stress-testing models, monitoring on-chain data, and blockchain analytics tools could help evaluate risks. Collecting off-chain data would also assist authorities to monitor important trends and behaviors, including forms of market manipulation or insider trading. Coordinating with developers on code reviews and audits could provide insights. Engaging with new governance models like DAOs will be key.</p>
<p>10. Do you find the interoperability between this report and the IOSCO CDA Report to be an effective overall framework? If not, please explain.</p>	<p>A nuanced decentralization spectrum between centralized and decentralized models may emerge, rather than a binary ecosystem. This perspective argues for an integrated series of recommendations on crypto-assets, stablecoins and DeFi, with the DeFi regime ideally less prescriptive and more a set of lenses on the crypto-asset recommendations.</p> <p>The IIF notes the abbreviated timeframe for responding to this consultation, and also duly notes that IOSCO has highlighted that these recommendations are complementary to those of the prior consultative report on crypto and digital asset markets. The IIF would suggest a subsequent period of public consultation would be prudent to consider IOSCO’s full set of proposed recommendations to understand and address the implications of their combination.</p>

Annex 2 – Comments on the Recommendations and Guidance

Page	Recommendation or guidance	IIF comment
	SECTION II. STATE OF THE DEFI MARKET	
5	Each jurisdiction should apply the IOSCO Standards, as they deem appropriate, within their existing or new frameworks.	As we commented in our July 31 submission ²⁰ to IOSCO on crypto-assets and stablecoins, we consider that the expression “as they deem appropriate” may leave an undesirable level of optionality. We would suggest “in the manner they deem appropriate” would make it clearer that jurisdictions are urged to implement the Recommendations, but the manner of implementation is a matter of discretion.
7, fn 11	The term stablecoin does not denote a distinct legal or regulatory classification.	We note that in some jurisdictions there are terms that map closely onto the concept of stablecoin, such as (in the EU) Asset-Referenced Token and (in Singapore) MAS-regulated stablecoins.
	SECTION III. RECOMMENDATIONS AND GUIDANCE	
19	<p>Recommendation 1. Analyze DeFi products, services, arrangements, and activities to assess regulatory responses</p> <p>A regulator should analyze DeFi products, services, arrangements, and activities occurring or located within its jurisdiction with a view to applying its Existing Framework or New Framework, as appropriate, in accordance with the principle of “same activity, same risk, same regulatory outcome.” To do so, a regulator should aim to achieve a holistic and comprehensive understanding of such DeFi products, services, arrangements, and activities. A regulator should assess what technological knowledge, data, and tools the regulator needs to understand, and analyze DeFi products, services, arrangements, and activities to inform regulatory responses.</p>	
20	<p>[Guidance on Recommendation 1]</p> <p>The regulator should seek to understand the DeFi arrangement at the economic reality level, or the “enterprise level.” ... The regulator should seek to ascertain how the particular arrangement was developed and</p>	This type of analysis is likely to be quite demanding, particularly if the analysis is conducted at the individual business level rather than at the industry level. The approach to analysis should be tailored to adequately and appropriately address existing risk in the market.

²⁰ IIF (2023b), *op. cit.*

Page	Recommendation or guidance	IIF comment
	founded, promoted and funded, and how it is operated, used and maintained.	
20	A regulator should also seek to analyze the DeFi arrangement at the functional level.	The distinction between the “enterprise level” and the “functional level” is not particularly clear.
21	A regulator also could seek to analyze the DeFi arrangement at the technical level, if feasible. ... For example, regulators may seek to understand how the settlement layer blockchain operates, including what type of consensus mechanism the settlement layer uses, the concentration of participants in the consensus mechanism, and to what degree they may impact the functioning of a smart contract or protocol, including through the inclusion or ordering of transactions (in connection with maximal extractable value (MEV) strategies) or by exerting some other control over the DeFi arrangement.	As with the “enterprise level” analysis, this type of technical analysis is likely to be quite demanding, particularly if the analysis is conducted at the individual business level rather than at the industry level.
22	<p>Recommendation 2. Identify responsible persons</p> <p>A regulator should aim to identify the natural persons and entities of a purported DeFi arrangement or activity that could be subject to its applicable regulatory framework (Responsible Person(s)). These Responsible Person(s) include those exercising control or sufficient influence over a DeFi arrangement or activity.</p>	<p>Meeting this recommendation seems to require auditing and large-scale de-anonymization. We note that at present supervisory technology capabilities to effect de-anonymization of blockchain addresses are still nascent.²¹ We also note that de-anonymization may give rise to privacy law compliance issues, unless appropriate exceptions are used or crafted.</p> <p>DeFi presents challenges to regulators in terms of identifying responsible entities, as we discussed in our November 2022 staff paper on DeFi.²² A DeFi protocol may be associated with a foundation or DAO (incorporated or not), the governance token holders of which may seem a natural focus for supervision. However, we would caution that many or most token-holders in a DAO may not have sufficient interest to count as decision-makers. Simply having the status of being a token-holder is not sufficient.</p> <p>In that context, a key issue is what level of control or interest defines a responsible person? Different markets treat this differently in securities structures, which could set up inter-jurisdictional enforcement issues. As such, we would suggest that</p>

²¹ See, e.g. BIS Innovation Hub et al., (2023), [Project Atlas: Mapping the world of decentralised finance](#)

²² IIF (2022a), *op. cit.*

Page	Recommendation or guidance	IIF comment
		<p>supervisors will need to undertake deeper thinking here and address the amount/percentage of fractional voting interest and the rights that particular tokens bring with them, as well as the entity(s) that hold overriding administrator privileges (if any). IOSCO may also be able to build on concepts from the accounting or prudential supervision spaces in terms of control concepts.</p> <p>The present recommendations may be seen as “casting the net widely” and potentially extending the reach of financial regulation far beyond its normal bounds.</p> <p>There may accordingly be a case for imposing current financial regulations on DeFi players that provide access to specific DeFi protocols and act in a commercial manner. With such concrete steps, more clarity could be achieved in the market instead of waiting for a ‘big-bang’ regulation that is also internationally fully aligned.</p> <p>In addition, centralized intermediaries facilitating access to DeFi represent the more obvious actors to be brought under the regulatory scope compared to the activity of developing software or “truly decentralized” protocols. We believe that regulating these intermediaries, in conjunction with some of the regulatory measures outlined above, will ultimately enable policymakers to achieve an outcome where investors and consumers are protected, risk transmission mechanisms are appropriate risk management, and jurisdictions apply appropriate risk-weighted resources to countering illicit financial activity.</p> <p>A broader conception of responsible persons (covering developers, all token holders, and each liquidity provider) is likely unworkable in practice, as it could capture essentially anyone who has interacted with a DeFi protocol or token. This would be technically difficult to implement, both by those seeking to comply and for supervisors, certainly without accompanying standards for identity management. As a result, it would likely create incentives for regulatory arbitrage among key parts of DeFi network infrastructure.</p>

Page	Recommendation or guidance	IIF comment
		<p>In keeping with the principle of “same risk, same regulatory outcome”, the approach IOSCO takes here is consistent with other financial regulation regimes that identify approved, senior or responsible persons, such as in the UK, that require those persons to be fit and proper. Additionally, all employees of financial firms must also comply with codes of conduct to ensure individual accountability for actions undertaken. Therefore, it would follow that the same principle should apply to those in a DeFi “enterprise” ecosystem.</p> <p>Beyond employees of protocol operators, there may be a need to adjust the scope of responsible person regimes to capture entities or personnel performing such functions under non-traditional arrangements, such as outsourced, decentralized or heavily automated compliance functions.</p>
23	<p>[Guidance on Recommendation 2]</p> <p>When considering persons and entities that may be Responsible Persons, it is important to note that governance mechanisms currently used for DeFi arrangements are not self-implementing ... Code could also be designed and updated through the deployment of automated methodologies – including those that utilize artificial intelligence or other technologies. For such cases, the person or entity that is responsible for deploying or using such methodologies could also be considered in the assessment of Responsible Persons.</p>	<p>In our 2022 staff paper, we pointed out that some possible objects of regulation associated with DeFi projects included, <i>inter alia</i>, developers writing the code and the smart contract code itself. We also said that the last two possibilities are likely to be very controversial.</p> <p>Where code is developed which has both legitimate and illegitimate users, it is not clear why developers – as opposed to those who use the code – should be responsible. On the other hand, where code can only be used in an illegitimate way, there may be a good case to sanction developers, particularly where they can be identified more easily than other actors and where there are reasons to believe they may have substantial assets. That said, in jurisdictions (such as the U.S.) with constitutionally protected free speech, regulators will always have difficulty frontally sanctioning the expressive activity of publishing code (for example, on GitHub).²³</p>
24	<p>Recommendation 3. Achieve common standards of regulatory outcomes</p>	<p>We support the idea of pursuing the same regulatory outcome for similar risks.</p>

²³ IIF (2022a), *op. cit.*, at p. 40.

Page	Recommendation or guidance	IIF comment
	<p>A regulator should use Existing Frameworks or New Frameworks to regulate, supervise, oversee, and address risks arising from DeFi products, services, arrangements, and activities in a manner consistent with IOSCO Standards. The regulatory approach should be functionally based to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets.</p>	<p>Our November 2022 staff paper on DeFi highlighted the benefits of technology neutral regulation focused on consistent risk mitigation outcomes, rather than identical regulation. We note IOSCO’s use of the phrase “regardless of the technology that may be used to deliver financial products and services”. We understand this phrase to be synonymous with “technology neutrality”, and to be consistent with the principle of “same risk, same regulatory outcome.”</p>
30	<p>Recommendation 4. Require identification and addressing of conflicts of interest</p> <p>In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of DeFi products and services and other Responsible Persons, as appropriate, to identify and address conflicts of interest, particularly those arising from different roles and capacities of, and products and services offered by, a particular provider and/or its affiliates. These conflicts should be effectively identified, managed and mitigated. A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions. This may include requiring more robust measures such as legal disaggregation and separate registration and regulation of certain activities and functions to address this Recommendation.</p>	<p>Conflict of interest mitigation is necessary in DeFi markets, and disclosures of such should be required to meet appropriate standards – perhaps requiring tailoring for unique risks – regarding what is included and how it is reported. Disclosure requirements should be calibrated so as to keep retail or institutional clients adequately informed, and also designed so as to enable compliant automatic market making and for protocols to meet reporting requirements in a product area that is frequently cross-border. Disclosure by protocols may require the protocol to collect more personal information from associated persons than at present.</p> <p>By design, most participants have an interest in the protocol by virtue of staking. As such, accounting for all interests within a protocol may be an un-meetable threshold for many protocols. We would accordingly suggest there is a need for further guidance on how to identify a “material interest” and what information should be disclosed to protect clients in that regard.</p> <p>We would also suggest that IOSCO could undertake further thought around the types of combinations of services and activities that are available via protocols that might not be available in TradFi.</p> <p>In response to IOSCO draft recommendations on crypto-assets and stablecoins, we submitted, “Two activities not specifically called out that may give rise to conflicts are issuance of unbacked crypto-assets by a CASP that also trades in those crypto-assets;</p>

Page	Recommendation or guidance	IIF comment
		<p>and involvement of venture capital affiliates in on-market or other trading activities.”²⁴</p> <p>Noting that the same language is used in this Recommendation, we also submitted, “We would urge greater clarity in the Recommendation as to the circumstances in which ‘more robust measures’, particularly involving legal disaggregation, would be justified.”²⁵</p> <p>Both of these comments hold valid for Recommendation 4 in the present consultation.</p> <p><u>Comment on Recommendations 4 and 5</u></p> <p>While generally welcome, Recommendations 4 and 5 will present unique challenges to DeFi operations, which (broadly speaking) have operated outside the regulatory and supervisory purview, and presumably without significant compliance operations.</p> <p>IOSCO should be encouraged to allow such operations to explore highly automated or novel methods of delivering the same regulatory outcomes. That said, even if there are automated solutions to achieve risk identification, it is important that those who use those solutions do so as a tool, and not as a means to obfuscate their responsibility for managing those risks, and maintain adequate oversight, including through human, financial or information resources where needed.</p>
31	<p>[Guidance on Recommendation 4]</p> <p>Concerns around conflicts of interest are further heightened if the provider of the DeFi product or service is in a fiduciary or similar relationship with a user.</p>	<p>It would be helpful to clarify that those DeFi operations that handle client money or client assets, or which agree to act as agent or arranger, would normally, or at least often, be in a fiduciary or similar relationship with a user.</p>

²⁴ IIF (2023b), *op. cit.*, p. 7

²⁵ IIF (2023b), *op. cit.*, p. 6

Page	Recommendation or guidance	IIF comment
33	<p>[Guidance on Recommendation 4]</p> <p>Regulators should seek to hold a provider of a DeFi product or service responsible for identifying and, to the extent practicable, managing and mitigating the impact of MEV strategies.</p>	<p>The common understanding of MEV has moved beyond its initial definition of transaction ordering to cross-chain arbitrage and other similar arbitrages so the definition could be clarified.</p> <p>As for transaction ordering, this seems to be one area where authorities working could usefully undertake further work to clarify expectations and limits. Extraction of MEV is somewhat akin to front-running or insider trading in more traditional financial markets. It is not clear why it should be tolerated, other than the pragmatic arguments around lack of enforceability (e.g. no node on a public permissionless network will see all the mempool containing all transactions or know the order in which they were added) and the important fact that, in many blockchains, these extractions reward essential notarial services. There are technical solutions to reduce impact, like batching using private mempools on a public blockchain for whitelisted participants or DEXs which use batch auctions to directly match. A severe possible response would be banning MEV extraction outright, forcing blockchain operators to embrace different business models (e.g. payment fees or tokens) to reward those services.</p>
33	<p>Recommendation 5. Require identification and addressing of material risks, including operational and technology risks</p> <p>In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of DeFi products and services and other Responsible Persons, as appropriate, to identify and address material risks, including operational and technology risks. These risks should be identified and effectively managed and mitigated. A regulator should consider whether certain risks are sufficiently acute that they cannot be effectively mitigated and may require more robust measures to address this Recommendation.</p>	<p>Materiality is poorly understood in DeFi. Technology risks could come from interactions between layers of the technology stack associated with a particular DeFi protocol or service. This both raises the issue of understanding composable technology elements, and how regulatory requirements should respond to providers and users of third-party services.</p>
34	<p>[Guidance on Recommendation 5]</p> <p>A provider of DeFi products and services can rely significantly upon oracles and cross-chain bridges for interoperability with off-chain data or other blockchains. When this is the case, a regulator should consider</p>	<p>If taking this approach, regulators should be urged to align with the principles of “same risk, same regulatory outcome” and technology neutrality, so as to enable an appropriately tailored</p>

Page	Recommendation or guidance	IIF comment
	applying identification, management, and mitigation measures similar to those applied to Responsible Persons in traditional finance, even if certain functionality has been outsourced to affiliated or unaffiliated service providers	regulatory framework and requirements for the risk posed by the underlying activity.
35	<p>Recommendation 6. Require clear, accurate, and comprehensive disclosures</p> <p>In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of DeFi products and services and other Responsible Persons, as appropriate, to accurately disclose to users and investors comprehensive and clear information material to the products and services offered in order to promote investor protection and market integrity.</p>	<p>Here IOSCO recommends identifying “lines of responsibility and accountability” to disclose and identify key persons. In our understanding, enforcement here would require digital signatures or other verified identities, which many markets are still working towards accepting.</p> <p>These Recommendations each deal with repairing information asymmetry and promoting consumer education from different angles. The recommendations, in effect, place the education and information burden on firms, rather than putting the onus on the client. For certain types of sophisticated or complex investment offerings in many jurisdictions, offering or investment requires the client to have a professional investor designation. There is no detail offered here on specifying level of education IOSCO is assuming or the type of disclosures other than they should be “plain language”. It would be helpful if the Recommendations were accompanied by some guidance on how disclosures could be tailored to the respective client cohort, e.g. retail vs. institutional clients, to ensure they are fit for purpose. We note the Recommendations should also require that relevant disclosures be updated when the position changes, to align with the crypto-assets and stablecoins recommendations. We recommend a materiality threshold be built in such that minor changes in role are not required to be disclosed.</p> <p>Also, we would note that, in our July 31 submission²⁶ to IOSCO on crypto-assets, we said that, ‘in the case of Bitcoin and Ether, and other similarly decentralized cryptocurrencies, it is not apparent which entity is the “issuer” concerned, in respect of which the [crypto-asset service provider] should disclose ‘full information</p>

²⁶ IIF (2023b), *op. cit.*

Page	Recommendation or guidance	IIF comment
		<p>about the issuer and its business, including audited financial statements’.</p> <p>It will be important for regulators to establish an enterprise view of the ecosystem, with the objective of identifying responsible persons who, depending on their function, will be involved in providing these disclosures. This is not inconsistent with approaches being taken in Hong Kong and the United Kingdom, for example.</p>
36	<p>Recommendation 7. Enforce applicable laws</p> <p>A regulator should apply comprehensive authorization, inspection, investigation, surveillance, and enforcement powers, consistent with its mandate, to DeFi products, services, arrangements, and activities that are subject to Existing Frameworks and New Frameworks, including measures to detect, deter, enforce, sanction, redress and correct violations of applicable laws and regulations. A regulator should assess what technological knowledge, data and tools the regulator needs to enforce applicable laws.</p>	<p>In our staff paper on DeFi, we referred to possible supervision strategies like embedded supervision, and assessing capabilities to oversee complex DeFi activities.²⁷ These could complement IOSCO’s call for consistent oversight.</p> <p>At the same time, we would caution that, while regulators may gear-up to supervise DeFi, including by engaging private sector actors who may be able to provide blockchain analytics, oracles, or other advanced data sources, any “embedded supervision” strategies should not blur lines of responsibility between actions and reports the regulator is responsible for and those that are the responsibility of regulated firms or other actors within the scope of regulation. In some jurisdictions there are breach reporting requirements which may need to be tailored for DeFi protocols.</p>
37	<p>Recommendation 8. Promote cross-border cooperation and information sharing</p> <p>A regulator, in recognition of the cross-border nature of DeFi products, services, arrangements, and activities, should have the ability to cooperate and share information with regulators and relevant authorities in other jurisdictions with respect to such arrangements, and activities. This includes having available cooperation and information sharing arrangements and/or other mechanisms to engage with regulators and relevant authorities in other jurisdictions. These should accommodate the authorization and on-going supervision of</p>	<p>Cross-border cooperation is essential for appropriate regulation and supervision of DeFi. As written, this Recommendation encourages coordination in information sharing and enforcement cooperation. We would note that information shared between authorities may need to be more comprehensive than is tackled in current information sharing arrangements, which should be acknowledged in this Recommendation. DeFi structures, the complexity of which is discussed in various papers, may mean that different actors or responsible entities are too scattered to realistically operate as desired under the suggested information</p>

²⁷ IIF (2022a), *op. cit.*

Page	Recommendation or guidance	IIF comment
	regulated persons and entities and enable broad assistance in enforcement investigations and related proceedings.	<p>sharing arrangements. The implications of this should be evaluated.</p> <p>Effective supervision of DeFi may also require a greater ability of authorities to share information relevant to supervision or enforcement activities in another jurisdiction, even if the responsible entity in question is not under supervision or investigation in their resident jurisdiction.</p> <p>We have consistently advocated for data free flow with trust, which in the regulatory context also includes the ability for regulators to share data with other regulators, and we continue to advocate for standardized information sharing “gateways” to address information barriers, through purpose-limited B2B, B2G and G2G data sharing, for example in the context of cross-border payments.²⁸</p> <p>We have also stated that supervisory colleges that already exist for certain systemically financial market infrastructures such as CCPs, and other ad-hoc arrangements such as those that oversee the Society for Worldwide Interbank Financial Telecommunication (SWIFT), may provide important models for cooperative oversight of a global stablecoin arrangement.²⁹ Important decentralized stablecoins, such as the Dai, may be suitable candidates for such supervisory approaches.</p>
39	<p>Recommendation 9. Understand and assess interconnections among the DeFi market, the broader crypto-asset market, and traditional financial markets</p> <p>When analyzing DeFi products, services, arrangements, and activities, a regulator should seek to understand the interconnections among DeFi arrangements, the broader crypto-asset market, and also the traditional financial markets. In so doing, a regulator should consider how those interconnections impact risks to investor protection and market</p>	<p>We welcome this emphasis on regulator responsibility for system-wide monitoring, building on the useful and important work of the OECD, FSB and IOSCO in this space.</p> <p>Monitoring linkages between DeFi and TradFi is important. Going one step further, one might suggest that this space would only become “mainstream” or exhibit its full potential if traditional or real-world assets are being effectively tokenized / deployed on efficient DeFi arrangements.³⁰ In such a system,</p>

²⁸ See IIF (2022b), *op. cit.*, p. 5; FSB (2023b), *op. cit.*, p. 15

²⁹ IIF (2022), [Submission to FSB on crypto-assets and global stablecoins](#), p. 15

³⁰ Aramonte et al. (2022), [DeFi lending: intermediation without information?](#), BIS Bulletin No 57

Page	Recommendation or guidance	IIF comment
	<p>integrity, and how they might identify further regulatory touchpoints, including potential responsible persons. A regulator should, as appropriate, seek to employ, maintain and develop suitable methods for monitoring and assessing DeFi products, services, arrangements, and activities.</p>	<p>TradFi institutions have the potential to act as effective risk managers and to provide / allocate liquidity where required.</p>