

Guidance consultation

Decentralised Finance (DeFi)

GC26/7

21 October 2026

1 Introduction

Why we are consulting

- 1.1 Firms are increasingly using decentralised finance (DeFi) to provide financial services. DeFi may support innovation and efficiency, but firms must continue to meet the same regulatory outcomes as are expected in traditional financial services. These include protecting consumers, maintaining market integrity, supporting operational resilience and managing financial crime risks. Firms using DeFi should do so safely and responsibly, as with other technologies.
- 1.2 We are consulting on non-Handbook guidance to help firms understand how existing operational resilience and financial crime requirements may apply when they provide financial services using DeFi.

Who this applies to

- 1.3 This consultation will be relevant to FCA regulated firms that interact with, facilitate access to, or provide financial services using DeFi, and that are subject to:
 - SYSC 15A (Operational resilience)
 - SYSC 6 (Compliance, internal audit and financial crime)
 - The Money Laundering Regulations (MLRs)

1.4 The requirements that apply will depend on the specific regulated activities a firm is carrying on. Firms should identify which FCA and legislative requirements apply to them before using this guidance.

1.5 It may also interest:

- other FCA regulated firms
- those who are not authorised by the FCA but interact with DeFi
- industry groups and trade bodies
- professional advisers
- consumers and groups representing consumer interests
- policy makers and other regulatory bodies
- academics and think tanks
- industry experts and commentators

How this links to our objectives

1.6 The proposed guidance supports our objectives of securing an appropriate degree of consumer protection, protecting and enhancing the integrity of the UK financial system, and promoting effective competition in the interests of consumers. It seeks to help firms identify and manage the risks arising when they provide financial services using DeFi.

Environmental, social and governance considerations

1.7 In developing this proposed guidance, we have considered:

- the environmental, social and governance (ESG) implications of our proposals
- our duty under section 1B(5) and 3B(1)(c) of the Financial Services and Markets Act 2000 (FSMA) to have regard to:
 - the net-zero emissions target under section 1 of the Climate Change Act 2008
 - environmental targets under section 5 of the Environment Act 2021

1.8 We do not consider that our proposals are relevant to those targets.

Equality and diversity considerations

1.9 We do not think our proposals materially affect any of the groups with protected characteristics under the Equality Act 2010 (in Northern Ireland, the Equality Act is not enacted but other antidiscrimination legislation applies).

Costs and benefits of our proposals

1.10 Section 138I of FSMA requires us to perform a cost benefit analysis for new rules, but not for guidance. The proposed guidance seeks to clarify existing rules rather than establish new policy. Therefore, we do not expect it to result in materially different costs or benefits.

Next steps

- 1.11 The consultation period will run from 21 October 2026 until 18 November 2026.
- 1.12 We will consider feedback and update the proposed guidance as appropriate. We plan to publish the final guidance in Q1 2027.

How to respond

- 1.13 Please respond by 18 November 2026. If you do not agree with our proposed guidance, we would welcome detail on your concerns and potential solutions.
- 1.14 You can submit responses through the [form](#) on our website or by email to GC26-7@fca.org.uk. If responding by email, please tell us if:
 - you want us to treat your response as confidential
 - you are content to be named as a respondent

Consultation questions

- Q1:** Do you agree with our description of the operational resilience risks that may arise when firms provide financial services using DeFi? If not, please explain why.
- Q2:** Do you agree with our proposed guidance on how firms should assess and manage those operational resilience risks? Are there other risks or emerging practices we should consider?
- Q3:** Do you agree with our description of the financial crime risks that may arise when firms provide financial services using DeFi? If not, please explain why.
- Q4:** Do you agree with our proposed guidance on how firms should assess and manage those financial crime risks? Are there other risks or emerging practices we should consider?
- Q5:** Are there other risks or emerging practices related to DeFi which we should consider?
- Q6:** Are there other steps that could be taken to reduce financial crime risks in DeFi? Are there other regulatory measures that we should consider to reduce the financial crime risks in DeFi?

Annex 1 Draft non-Handbook guidance on Decentralised Finance (DeFi)

1 Introduction

What is DeFi?

- 1.1 Decentralised finance (DeFi) refers to financial services (such as trading, lending and borrowing) facilitated by use of distributed ledger technology (DLT), including blockchain networks and smart contracts, and that typically:
 - use smart contracts to automate transactions and processes
 - use open and interoperable technology
 - may operate with limited or no involvement from traditional intermediaries.
- 1.2 DeFi is most prevalent in the cryptoasset ecosystem and is commonly used for activities also undertaken in traditional finance and centralised finance (CeFi). Firms may also use DeFi to provide broader financial services in emerging use cases, including tokenised financial markets and agent payments.
- 1.3 Some FCA regulated firms, and persons that may become authorised under the future cryptoasset regime, are already using or interacting with DeFi. This includes facilitating client access to decentralised protocols, executing transactions through decentralised exchanges, and participating in decentralised liquidity, lending and staking.

Market development, benefits and risks

- 1.4 Nonetheless, consumer and market engagement with DeFi is currently relatively limited. Between January and August 2026, trading on decentralised exchanges represented approximately 14% to 19% of global cryptoasset spot trading volume. FCA research found that, in 2025, around 8% of UK cryptoasset users acquired cryptoassets through decentralised exchanges. However, the use of DeFi may increase as the cryptoasset regulatory regime is implemented, potentially increasing firms' and consumers' exposure to its benefits and risks.
- 1.5 Used appropriately, DeFi may support innovation, efficiency and broader market access. Its potential benefits include:
 - **Automation and efficiency:** smart contracts can automate transactions and business processes.
 - **Continuous access:** some services and markets can operate outside traditional trading hours.
 - **Potential for broader access:** open networks can allow a wider range of users to access services, subject to applicable legal, technical and commercial restrictions.
 - **Composability and innovation:** protocols can interact with one another to support new products and services.

1.6 DeFi can also create or amplify risks that might otherwise be managed by traditional intermediaries. These include risks relating to governance, accountability, consumer protection, operational resilience and financial crime. For example:

- **Smart contract vulnerabilities:** coding errors, security weaknesses or manipulation can result in financial loss or service disruption.
- **Limited consumer recourse:** transactions are difficult to reverse, and there may be no central authority able to recover assets or compensate consumers.
- **Loss or compromise of private keys:** compromised credentials can result in the loss of, or unauthorised access to, cryptoassets.
- **Oracle failures:** inaccurate, delayed or manipulated external data can cause smart contracts to produce unintended outcomes.
- **Fraud, scams, money laundering and other financial crime and sanctions risks:** consumers could be exposed to fraudulent projects, malicious code and deceptive practices, and DeFi could be used by illicit actors.
- **Complex dependencies:** failures affecting protocols, networks, bridges, data providers or other infrastructure can disrupt multiple interconnected services.

1.7 Industry data indicates that these risks can crystallise. More than US\$12bn has reportedly been lost through DeFi and bridge hacks since 2016. The nature and significance of the risks will depend on a firm's activities, business model and the way in which it uses or interacts with DeFi.

Firms' responsibilities

1.8 Firms remain responsible for complying with applicable legal and regulatory requirements when they use or interact with DeFi. They should assess whether they can adequately identify, understand, manage and mitigate the risks arising from a proposed activity. Where they cannot do so adequately, they should consider whether the activity is appropriate for their business and clients.

1.9 Those providing financial services using DeFi should also consider whether they are carrying on a regulated activity by way of business in the UK for which they need to be authorised or exempt. The use of software, smart contracts, DLT or other decentralised arrangements does not, by itself, determine whether an activity is regulated.

Purpose and scope of this guidance

1.10 This guidance is intended to help firms identify, assess and manage operational resilience and financial crime risks when providing financial services using DeFi.

1.11 This guidance does not create new regulatory requirements. It explains how existing FCA requirements relating to operational resilience and financial crime may apply when firms use or interact with DeFi. It also provides observations on the current risk landscape and illustrative examples of measures firms may wish to consider when designing or enhancing their systems and controls. These examples (including risk management and emerging industry compliance practices) are not exhaustive and may not be appropriate in every case.

1.12 In this guidance, "must" describes an existing legal or regulatory requirement. "Should" indicates guidance on how firms may meet or consider those requirements.

1.13 The guidance is primarily intended for FCA-authorised firms that use or interact with DeFi as part of their regulated activities, including firms carrying on future regulated

cryptoasset activities. It will also be relevant to firms seeking authorisation and may be useful to other firms that use or interact with DeFi, including firms engaging with tokenised assets.

- 1.14 Firms might interact with DeFi in different ways, including receiving cryptoassets transferred by clients, partnering with firms that use DeFi, or engaging directly with DeFi protocols. Firms should assess the risks arising from their particular business model and ensure these are reflected in their risk management and business-wide risk assessments, including those required under the MLRs.
- 1.15 Moreover, DeFi continues to evolve rapidly, and the risks associated with it are also likely to change. Firms should therefore consider how developments in DeFi from technology, products and business models may affect their activities, risk profiles and regulatory obligations.

Related publications

- 1.16 This guidance should be read alongside [CP26/36](#) and [PS26/18](#), which provide further information on decentralisation, the scope of regulated cryptoasset activities and when authorisation may be required.
- 1.17 Firms may also find our wider publications on the [cryptoasset regime](#), [financial promotions](#) and the [Consumer Duty](#) helpful when considering how to comply with applicable requirements. Our publications on [operational resilience](#) and our [Financial Crime Guide](#) (FCG) are also relevant.

2 Need for authorisation

- 2.1 Decentralisation may affect whether a person needs to be authorised or exempt when they carry on a regulated activity in the UK by way of business. [PS26/18](#) and [CP26/36](#) set out considerations that may be relevant to this assessment and explain how decentralisation can affect perimeter analysis.
- 2.2 However, the approach to perimeter analysis remains the same regardless of how a business model is described (for example as centralised, decentralised or DeFi). As set out in [CP26/36](#), persons carrying on a regulated activity by way of business in the UK, and in respect of which no exclusion applies, will need to be authorised or exempt, even if they describe themselves as DeFi. Even where a firm meets the conditions of an exclusion from a regulated activity, they must still consider whether their activities are within the scope of the financial promotions regime, or the [Money Laundering Regulations](#) (MLRs).
- 2.3 [CP26/36](#) also explains that the use of software, smart contracts, DLT, distributed governance mechanisms or other technological arrangements does not, by itself, determine whether a person is carrying on a regulated activity. Firms should refer to [PS26/18](#) and the draft guidance in [CP26/36](#) for further information on how decentralisation may affect perimeter analysis.

3 Operational resilience

3.1 This chapter sets out:

- operational resilience and technological risks firms may face when providing financial services using or interacting with DeFi
- emerging practices on maintaining operational resilience
- guidance on applying [SYSC 15A](#) requirements

3.2 Various FCA-regulated firms, including all cryptoasset firms from October 2027, must comply with the requirements in SYSC 15A. These requirements apply irrespective of whether the firm uses or interacts with DeFi.

3.3 All firms interacting with DeFi or providing services themselves using DeFi should understand the operational and technological risks of DeFi, and how they can manage and mitigate them to protect consumers from harm and maintain market integrity. This is a requirement for various firms, including those subject to SYSC 15A.

3.4 When considering these operational and technological risks, firms should also consider our non-Handbook guidance on operational resilience for cryptoasset firms ([FG26/6](#)) and our future guidance consultation covering use of DLT. This will help firms consider how our operational resilience requirements can apply in practice for business models involving use of DLT.

Our other operational resilience standards

3.5 As well as SYSC 15A, firms should consider other parts of the FCA Handbook as relevant. This includes, but is not limited to:

- Principles for Business (PRIN)
- [SYSC 3](#) (Systems and Controls)
- [SYSC 4](#) (General Risk Management Requirements)
- [SYSC 7](#) (Risk Control)
- [SYSC 8](#) (Outsourcing)
- [SUP 15](#) and [SUP 16](#) (Operational Incident and Third Party Reporting).

3.6 Firms are responsible and accountable for all the regulatory responsibilities that apply to outsourcing and third-party service arrangements. Firms cannot delegate any part of this responsibility to a third party.

Risk landscape

3.7 Operational disruption affecting DeFi arrangements can prevent clients from accessing assets or services, cause transactions to fail or be delayed, and result in financial loss. Interdependencies between protocols, service providers and financial market infrastructure may also allow disruption to spread across firms and markets.

3.8 DeFi shares operational risks found elsewhere in financial services and the cryptoasset sector, including technology failure, cyber risk, third-party dependency and concentration risk. However, reliance on smart contracts, automated execution,

decentralised governance and interconnected protocols may change the nature, scale or speed of those risks.

- 3.9 Emerging technologies may also affect firms' operational resilience risk profile. For example, advances in AI, especially agentic AI, may strengthen firms' ability to identify, monitor and respond to risks, including those posed by interactions with DeFi. At the same time, AI could also increase the sophistication, speed and scale of cyberattacks. Firms should consider how technological developments could affect their operational resilience and risk management processes, and how to respond effectively.
- 3.10 Firms should consider whether their use of DeFi introduces additional risks, which may include:
- **Technology and protocol risk:** weaknesses or failures in the technology that supports DeFi, including smart contracts, bridges, data feeds (oracles), network design and transaction validation processes.
 - **Operational and governance risk:** uncertainty about who is responsible for managing risks and responding to incidents in decentralised ecosystems, and the complexity created by interconnected protocols and service providers.
 - **Security risk:** cyberattacks, financial crime, sanctions evasion and exploitation of vulnerabilities.
 - **Third-party risk:** dependence on external providers, infrastructure and data sources.
 - **Incident management risk:** challenges in detecting, responding to and recovering from disruptions.
- 3.11 Below are examples of existing risks, which firms can use to consider how their particular use of, or interaction with, DeFi may affect their operational resilience. Firms should consider carefully the risks posed by their own business model and their interaction with or use of DeFi.

<i>Risk Category</i>	<i>Examples</i>
<i>Infrastructure and system risk</i>	• Firms may rely on open-source code that they do not control, making it harder to address faults or implement critical fixes quickly. • DeFi generally operates on public blockchain networks, which can experience congestion, delays or transaction failures. Network disruptions or changes to transaction records can affect the accuracy and reliability of transactions.
<i>Security and cyber risk</i>	• DeFi often relies on interconnected components, such as wallets, bridges and data providers. A failure or attack affecting one component can disrupt multiple services. • Smart contract code is often publicly available, allowing vulnerabilities to be identified and exploited by malicious actors. Similar weaknesses can affect multiple protocols where the same code is reused.

<i>Risk Category</i>	<i>Examples</i>
<i>Interoperability and integration failure</i>	• Changes to protocols or supporting infrastructure can disrupt connected services, resulting in failed transactions or inaccessible assets. • Failures in the links (eg APIs, middleware) between centralised and decentralised systems can interrupt transaction processing and settlement.
<i>Third-party dependency risk</i>	• Firms might depend on third-party infrastructure and service providers to support critical functions. Outages or performance issues at these providers can disrupt client access and transaction execution.
<i>Monitoring and response risk</i>	• Smart contracts may be difficult to pause, amend or reverse after deployment, limiting a firm's ability to stop or correct a problem. • Reliance on real-time data means inaccurate, delayed or unavailable information can cause controls to fail. • Decentralised operating models can make it harder to identify responsibility, detect incidents and coordinate an effective response.

Case studies

- 3.12 Case studies 1 to 3 provide recent real-world examples of operational and technology-related disruptions that can arise when a business model involves decentralisation, and the potential harm to consumers. These examples are illustrative only for the purposes of highlighting the importance of complying with SYSC 15A requirements.
- 3.13 Our rules in SYSC 15A aim to help firms prevent, adapt to, respond to, recover from and learn from operational disruptions. Nonetheless, operational resilience measures cannot prevent every disruption or instance of harm, making it critically important for firms to understand their own businesses and how they have applied our requirements. Firms should consider how they would respond to comparable events and be able to continue delivering important business services within their impact tolerances. This includes considering the resources needed to respond and recover, and how the firm would communicate with clients and other stakeholders.

Case Study 1: Security and cyber risk, and monitoring and response risk: KelpDAO/LayerZero bridge attack

In April 2026, hackers from the OFAC-designated, North Korea-controlled Lazarus Group exploited a security weakness in the LayerZero OFT bridge, which is used by the re-staking protocol KelpDAO, to steal over US\$290m in cryptoassets. The bridge used a single-verifier configuration, instead of a more secure multi-verifier setup. Since DeFi relies on interconnected components, KelpDAO inherited this security vulnerability.

The attackers also exploited monitoring and detection gaps in KelpDAO itself. They fed false data to the LayerZero bridge's internal RPC nodes and simultaneously launched a distributed denial-of-service (DDoS) attack on external nodes. This meant the on-chain transaction appeared to be valid and

part of normal bridge activity, and KelpDAO's security tools could not detect the attack.

The hackers used the stolen cryptoassets as collateral to borrow US\$190m on the Aave protocol, causing Aave depositors to lose confidence and withdraw over US\$10bn. The knock-on impact on consumers and the DeFi market was severe. In the two days following the attack, the total value locked in DeFi protocols dropped by US\$13bn.

Case Study 2: Security and cyber risk: Polygon Plasma Bridge bug bounty

In October 2021, the Polygon network ran a bug bounty programme to look for security vulnerabilities in its software. It found a flaw in its Plasma Bridge that could have allowed an attacker to submit the same withdrawal transaction 224 times. An attacker could have exploited this to deplete the entire US\$850m held by Plasma Bridge through multiple fraudulent transactions.

Polygon created and tested a fix, then deployed it on the main Polygon network.

Case Study 3: Infrastructure and system risk: Sui Network outage

In January 2026, the Sui network had a major outage in its core infrastructure and had to pause transactions for six hours. The disruption was caused by a bug that caused internal divergence in validator consensus processing.

Sui halted transaction processing and warned its users of the outage so they did not lose funds. Sui resumed operation after validators deployed a fix and reprocessed consensus data. However, over US\$1bn in on-chain value was inactive during the outage, blocking consumers from accessing their cryptoassets during that time.

Emerging practices to support operational resilience

- 3.14 Where firms use DeFi to provide financial services, they should consider how they can maintain operational resilience throughout the lifecycle of a product or service. This could include:
- **Building resilience into system design**, for example through appropriate controls, safeguards and contingency mechanisms.
 - **Testing systems before deployment**, including assessing how they perform under a range of severe but plausible scenarios.
 - **Managing technology and security risks**, including identifying vulnerabilities and addressing them in a timely manner.
 - **Monitoring services on an ongoing basis**, including dependencies on third parties and critical infrastructure.
 - **Detecting, reporting and responding to incidents effectively**, including considering how risks may spread across interconnected services and markets.
- 3.15 The appropriate approach will depend on the firm's business model, activities and risk profile.

Assessing and managing DeFi risks in the context of our operational resilience framework

- 3.16 DeFi-related risks can affect a firm's operational resilience and its ability to deliver important business services within impact tolerances.
- 3.17 SYSC 15A requires in-scope firms to identify important business services, map resources, set impact tolerances, and plan and test severe but plausible disruption scenarios.
- 3.18 We use two fictional example firms below to illustrate how different aspects of our operational resilience requirements could apply when a firm uses DeFi as part of its regulated activities. These examples may also be helpful for firms not FCA-
authorised whose business models involve decentralisation.

Important business services

- 3.19 Under [SYSC 15A.2.1 \[R\]](#), firms must identify their **important business services**: services where disruption could cause intolerable harm to their clients or threaten UK market integrity or financial stability.
- 3.20 Firms should identify the service delivered to the client, rather than treating the underlying technology or protocol as the important business service. Depending on the firm's activities, relevant services could include enabling clients to trade, transfer, lend, borrow or stake cryptoassets.
- 3.21 Under [SYSC 15A.2.5 \[R\]](#), firms must set an **impact tolerance** for each important business service, defining the maximum level of disruption they can tolerate before harm occurs.
- 3.22 When setting impact tolerances, firms should consider factors relevant to their use of DeFi, such as:
- clients being unable to access, transfer or transact with assets
 - failed, delayed or reversed transactions
 - inaccurate pricing or data failures
 - assets becoming inaccessible or exposed to further risk of operational disruptions or hacking
- 3.23 Firms should also consider the non-exhaustive list of factors set out in [SYSC 15A.2.7 \[G\]](#).
- 3.24 This example shows how a firm might identify important business services and set impact tolerances:

Firm A: Firm arranging staking of a client's cryptoassets via decentralised protocols (see also article 926 of the Cryptoasset Regulations)

Firm A is regulated to provide staking services and offers a service that stakes clients' cryptoassets via decentralised protocols to earn yield. It selects liquid staking protocols based on defined risk, resilience and performance criteria. The staking protocols select third-party validator node operators.

Firm A identifies the provision of its staking service, including its selection and use of decentralised protocols, as an important business service. It identifies examples

of disruptions that could cause intolerable harm, such as vulnerabilities in the selected staking protocol or connected protocols, disruption to the underlying network, and outages affecting validator node operators. These events could lead to slashing losses or prevent the firm from returning clients' cryptoassets, disrupting the service.

The firm considers the number of affected clients, the monetary value of clients' losses, and the length of time the service is inaccessible to clients when setting its impact tolerances.

Mapping requirements

- 3.25 Under SYSC 15A.4.1 [R], firms must map the people, processes, technology, facilities and information that support their important business services. This must be sufficient to allow the firm to identify vulnerabilities and remedy these as appropriate.
- 3.26 For firms using DeFi, this should include key dependencies and supporting controls. Firms should have a sufficient understanding of any third parties or external dependencies that support service delivery, in line with SYSC 15A.4.2 [G].
- 3.27 Mapping may include:
- the underlying DLT and settlement infrastructure
 - cloud and technology providers
 - external protocols, smart contracts and middleware (such as oracles and bridges)
 - client-facing interfaces
 - internal functions, including incident response, key management, governance, oversight and client communications
- 3.28 Firms should also identify governance arrangements (eg for protocol upgrades and emergency controls) and change-control (eg admin keys) mechanisms that could affect the delivery of important business services.
- 3.29 This example shows how a firm might approach the mapping exercise:

Firm B: Offering a non-custodial wallet

Firm B provides a number of regulated financial services as well as access to DeFi through a non-custodial wallet. This allows clients to hold cryptoassets, sign transactions, and swap cryptoassets. The firm takes steps to ensure that orders from UK retail clients and UK elective professional clients are executed on a UK qualifying cryptoasset execution venue.

To manage operational resilience, the firm maps the interdependencies that support each of its important business services. This includes the oracles it relies on to estimate network transaction fees, and the DEX aggregators (which aggregate liquidity data and allow order execution across multiple DEXs) it uses to offer users the best swap prices.

The firm also maps the controls and processes that support the service, such as the mechanisms that support independent verification of balances and transactions.

Scenario planning and testing

- 3.30 SYSC 15A.5.1 [R] requires firms to develop a testing plan and carry out scenario testing to assess whether they can remain within their impact tolerances during severe but plausible disruption.
- 3.31 For firms using DeFi, this may include testing the impact of failures affecting DLT infrastructure, cloud or technology providers, smart contracts, third-party services, data feeds, bridges, and client-facing interfaces.
- 3.32 Under SYSC 15A.5.5 [G], where firms rely on third parties for the delivery of their important business services, they should work with the third parties to ensure the validity of the firm's scenario testing. If third parties carry out tests on behalf of the firm, the firm should ensure the suitability of the methodologies, scenarios and considerations adopted by the third party in carrying out testing. The firm is ultimately responsible for the quality and accuracy of any testing carried out, whether by itself or by a third party.
- 3.33 Following testing or an operational disruption, in line with SYSC 15A.5.8 [R], firms must conduct a lessons-learned exercise to identify weaknesses, make improvements, and support ongoing resilience.
- 3.34 This example shows how a firm could approach scenario planning and testing:

Firm B: Offering a non-custodial wallet

As part of its operational resilience testing, Firm B assesses whether it can continue to deliver its non-custodial wallet service during severe but plausible disruptions, including:

- outages affecting key wallet infrastructure
- failures affecting transaction signing or submission
- inaccurate or unavailable network fee information
- loss of connectivity to third-party RPC node providers

The firm tests its ability to continue providing important business services, communicate effectively with clients, and manage failed or delayed transactions.

Testing identifies weaknesses in the firm's resilience arrangements. The firm makes improvements, including reducing reliance on a single RPC node provider, and retests to ensure it can remain within its impact tolerances.

Communication strategies

- 3.35 Under SYSC 15A.8.1 [R], firms must maintain communication strategies that enable them to respond quickly and effectively to operational disruption.
- 3.36 Firms using DeFi should consider how they will communicate with clients and other stakeholders during incidents, including through digital channels and client-facing interfaces. They should also have processes to gather relevant information and assess the impact of disruptions.
- 3.37 In line with SYSC 15A.8.3 [R], firms must provide clear, timely and relevant communications to ensure that clients are informed in the event of disruption. Where

relevant, firms may explain the nature of the disruption, likely impacts, potential limitations on remediation, and any actions clients can take to reduce harm.

- 3.38 Effective communication can help reduce harm, support incident management, and maintain trust during periods of disruption.

Third-party arrangements

- 3.39 Firms using DeFi might rely on protocols, infrastructure and service providers that they do not control. Firms in scope of SYSC 15A remain responsible for understanding and managing the risks these dependencies create for their important business services.
- 3.40 Firms in scope of SYSC 15A must:
- map key dependencies and their role in service delivery
 - understand any limits on their ability to control or recover from disruptions impacting third-party services
 - monitor the performance and resilience of critical dependencies
 - test the impact of severe but plausible failures
 - assess concentration risk and the availability of alternatives
 - maintain clear communications with clients and regulators during incidents
- 3.41 Our operational resilience requirements (SYSC 15A) apply to relevant third-party arrangements whether or not they constitute outsourcing. Where they do constitute outsourcing, in-scope firms must also consider the applicable requirements in SYSC 8. Firms are responsible and accountable for all the regulatory responsibilities that apply to outsourcing and third-party service arrangements.

Reviewing compliance

- 3.42 Under SYSC 15A.2.2 [R], SYSC 15A.2.6 [R], SYSC 15A.4.3 [R] and SYSC 15A.5.7 [R], firms must review their compliance with operational resilience requirements following a significant change to their business, operating model or the markets in which they operate. They must keep their identification of important business services, impact tolerances, mapping and scenario testing under review to ensure they remain appropriate.

4 Financial crime

4.1 This chapter explains:

- financial crime risks that may arise when firms provide financial services using or interacting with DeFi
- emerging practices for mitigating those risks
- how firms should consider relevant obligations under SYSC 6 and the MLRs, where applicable

4.2 Firms should keep their assessment of financial crime risks up to date. Relevant risks may include fraud, scams, money laundering, terrorist financing, proliferation financing and sanctions evasion. Depending on the firm's activities, market abuse risks may also arise. Inadequate controls can expose firms and customers to financial loss and other harm, and increase the UK's exposure to financial crime risks.

4.3 This guidance does not replace the FCG and firms that are required to comply with SYSC 6 should read and apply that guidance in its entirety.

Risk landscape

4.4 The National Risk Assessment on Money Laundering and Terrorist Financing 2025 highlights a significant increase in money laundering using cryptoassets since 2020. Criminals might seek to exploit features of some DeFi arrangements, including limited customer identification, automated execution and complex cross-chain transaction flows, to conceal or move illicit funds.

4.5 FATF has similarly highlighted the growing financial crime risks associated with DeFi and noted that criminals, sanctioned entities and their associates increasingly use DeFi services, particularly where access to traditional financial services or centralised cryptoasset providers is restricted.

4.6 Firms interacting with DeFi could face heightened exposure to money laundering, terrorist or proliferation financing, sanctions evasion and other illicit finance risks where proportionate controls are not in place, or not up to date. This could lead to consumer harm, financial losses, market disruption and potential national security concerns.

4.7 DeFi has also been associated with significant losses from criminal and sanctions evasion activities. Industry analysis suggests that DeFi protocols continue to be a key route for laundering stolen cryptoassets. In addition to making use of conventional fraudulent or layering typologies, nefarious actors have exploited the inherent technical vulnerabilities of DeFi to raise, layer or move illicit funds. Recent incidents have involved both technical exploits, such as smart contract vulnerabilities, and off-chain attacks, including phishing, private key theft and compromised user interfaces.

4.8 Some of the key factors that could increase financial crime and sanctions risks include:

- **Technology and infrastructure risks**, such as cross-chain bridges, non-custodial wallets and anonymity-enhancing technologies.
- **Risks arising from decentralised protocols and ecosystem design**, including limited oversight, reduced customer verification and weaker transfer information controls.
- **People and governance risks**, including social engineering, exploitation of control weaknesses and differences in regulatory approaches across jurisdictions.

4.9 Firms should consider how the infrastructure, features and operating models associated with DeFi could be exploited for illicit purposes. For example, while cross-chain bridges can improve interoperability and liquidity, they may also make transaction tracing more difficult and create opportunities for illicit fund movements.

4.10 The table below sets out illustrative examples of financial crime risks associated with DeFi that firms interacting with DeFi should consider. As a start, firms should consider how criminals could exploit these and other vulnerabilities (including new and emerging ones) as part of complying with SYSC 6 and MLR requirements.

<i>Risk category</i>	<i>Examples</i>
<i>Technological infrastructure risks</i>	• Flash loans in DeFi enable large volumes of uncollateralised borrowing within a single transaction. Combined with the automation and speed of DeFi, this can enable malicious actors to manipulate markets or exploit vulnerabilities at scale, causing consumer losses and undermining market integrity. • Mempool transparency can expose pending transactions before they are confirmed. This creates opportunities for sandwich attacks, where actors manipulate transaction ordering to profit at users' expense. • Compared to centralised exchanges, the admission of new cryptoassets to trading on some DEXs may not involve the same level of approval or compliance controls. This can make it easier for fraudsters to launch cryptoassets or projects designed to facilitate scams, including rug pulls, resulting in consumer losses.
<i>Intermediary and control gaps</i>	• Responsibility for financial crime controls may be fragmented across developers, governance participants and infrastructure providers, creating potential gaps in AML/CTF/CPF controls. • Limited customer due diligence may make it harder to identify users and assess risk, increasing exposure to money laundering and sanctions evasion. • Automated transaction execution may reduce opportunities to identify and prevent suspicious activity. • Limited ability to intervene after execution may, depending on the circumstances, constrain asset recovery and other responses to financial crime.
<i>Anonymity and concealment risk</i>	• The speed, automation and composability of DeFi can help illicit actors move funds rapidly across multiple

<i>Risk category</i>	<i>Examples</i>
	chains as a layering and obfuscation technique, making it harder to track illicit fund flows. Equally, the use of agentic AI to undertake transactions can increase the scale and speed of fund flows. • Illicit actors can use, and are increasingly using, privacy-enhancing technologies, such as: – mixing services to pool and redistribute funds and break transaction trails – cross-chain bridges and swaps as a layering technique – privacy coins to obscure transaction details and hinder attribution
<i>Social engineering risk</i>	• Users may be targeted through phishing or other social engineering attacks, leading them to approve unauthorised transactions or grant access to their cryptoassets. • Protocols that rely on multiple approvals or decentralised governance may be vulnerable to social engineering, with attackers influencing participants to approve malicious changes that compromise controls or facilitate theft.
<i>Geographic and jurisdictional risk</i>	• Cross-border and multi-jurisdictional activity can make it harder to determine applicable regulatory obligations and assess the overall effectiveness of financial crime controls.

Case studies

- 4.11 Case studies 4 to 6 provide real-world examples of financial crime risks that can arise when a business model involves decentralisation, and the potential harm that may result to consumers. These examples are illustrative only, for the purposes of highlighting the importance of:
- carrying out appropriate financial crime risk assessments
 - maintaining risk-based systems and controls
 - applying customer due diligence and screening where required
 - conducting effective ongoing monitoring

Case Study 4: Protocol design risk, and anonymity and concealment risk: \$SQUID 'rug pull' scam

In 2021, anonymous developers created the \$SQUID token and made it available for trading through a liquidity pool on the DEX, PancakeSwap. They exploited the lack of oversight on the DEX to admit the cryptoasset without the review processes required by a CEX.

The price of \$SQUID surged by over 40,000% in the weeks following its launch. However, the smart contracts underpinning it were designed to allow only the

scammers to sell the cryptoasset. In November 2021, the scammers initiated a 'rug pull' scam, draining the liquidity pool and leaving \$SQUID worthless.

The scammers then used the OFAC-designated mixer Tornado Cash to launder the stolen funds and obscure their origin.

Blockchain analysis highlighted that the scammers behind \$SQUID were linked to two other rug pulls, stealing an estimated US\$19.3m in invested funds.

This case study illustrates the importance of assessing risks associated with newly issued cryptoassets and relevant protocols. When assessing the transaction patterns and their links to illicit or sanctioned activity, firms should consider the information available about those responsible for the type of cryptoasset or project, for example, the initial ownership and transaction history, especially for newly minted cryptoassets or newly launched projects.

Case Study 5: Intermediary and control gaps, and social engineering risk: Bybit UI-layer hack

In February 2025, hackers from the OFAC-designated, North Korea-controlled Lazarus Group stole US\$1.5bn in cryptoassets from Bybit. While Bybit is a CEX, hackers targeted the user interface of Safe Wallet, the free decentralised wallet software that Bybit used for its transaction and multi-signature process. They used a phishing attack to embed malicious code that made the transaction appear legitimate at the front-end to the Bybit employees required to approve the transfer, nullifying the security benefits of the multi-signature process.

The hackers also used decentralised infrastructure to rapidly launder the stolen cryptoassets, using DEXs to avoid the CDD of a CEX, and sending the funds to over 50 different non-custodial wallets as a layering tactic to complicate the tracing process.

The incident illustrates the importance of assessing risks arising from third-party interfaces and approval processes, and of monitoring attempts to move stolen assets through decentralised infrastructure. When assessing the risks in relation to their products, services and delivery channels, firms should consider if and how the use of third-party interfaces would amplify the identified risks, and whether the third-party interfaces have adequate risk-control measures before interacting with these interfaces.

Case Study 6: Social engineering risk: Solana Drift exploit

In April 2026, hackers linked to North Korea stole US\$285m in cryptoassets from Drift, the largest DeFi protocol on the Solana Network.

The attack was highly coordinated, involving a months-long off-chain social engineering campaign. The attackers posed as legitimate investors to establish relationships with members of Drift's administrator group with responsibility for approving its critical protocol upgrades and treasury actions. The attackers induced members to pre-sign malicious transactions that transferred administrative control of the protocol to the attackers, who then used a fake cryptoasset as collateral to withdraw legitimate cryptoassets. As the

transactions appeared legitimate, on-chain safeguards did not work. The protocol had also adopted a zero-timelock configuration, allowing administrative changes to take effect without a mandatory delay. This enabled the malicious changes to be executed immediately.

This attack was enabled by DeFi-specific governance structures, where key protocol functions are often approved through multi-signature signers and decentralised governance participants. Compromising a small number of these participants can give attackers significant administrative control, disrupting services and leading to theft of consumers' assets.

The attackers laundered the stolen cryptoassets by converting them to USDC, bridging these funds to Ethereum and swapping the USDC for ETH using DEXs.

This case study illustrates the importance of assessing a protocol's governance arrangements before integrating it into a firm's services. Relevant considerations may include the concentration of administrative control, transaction approval arrangements, timelocks and controls over critical changes.

Assessing and managing DeFi risks in the context of our financial crime framework

- 4.12 Firms authorised under FSMA must comply with our financial crime rules under SYSC 6, in addition to other financial crime legislation such as the MLRs where applicable. Providing financial services using DeFi does not automatically make firms non-compliant, but firms will need to consider the financial crime risks specific to DeFi. The FCG provides additional guidance to help firms implement appropriate controls.

Risk assessments

- 4.13 In line with [Regulation 18](#) and [18A](#) of the MLRs and FCG 2.2.4, firms must undertake a business-wide assessment of their exposure to money laundering, terrorist financing and proliferation financing risks.
- 4.14 In the context of DeFi, firms should consider whether the use of multiple protocols, smart contracts and services within a single transaction increases the complexity of transaction flows and makes it more difficult to identify participants and trace the source and destination of funds. Firms should take these risks into account when assessing their systems and controls.
- 4.15 As set out in FCG 3.2.3 and FCG 3.2.6, firms should consider the source of wealth and source of funds risks associated with a business relationship. Where transactions involve DeFi, firms should consider whether there are indicators of elevated risk. These may include exposure to services or entities associated with illicit activity, such as darknet markets, mixing services or sanctioned persons and services.

Systems and controls

- 4.16 As set out in [SYSC 6.3.1 \[R\]](#) and [SYSC 6.3.3 \[R\]](#), firms must establish and maintain proportionate policies and procedures to counter the risk that they might be used to further financial crime.
- 4.17 When assessing whether their systems and controls remain proportionate, firms should consider whether the risks specific to interaction with DeFi have been accounted for, such as whether:
- the products, services or protocols they use create additional opportunities for money laundering, terrorist financing, proliferation financing or sanctions evasion;
 - the channels through which customers access services make it more difficult to identify or manage financial crime risks;
 - complex transaction flows across multiple protocols or blockchain networks make monitoring and investigation more challenging;
 - their systems and controls are capable of identifying exposure to illicit activity linked to wallet addresses, smart contracts or protocols; and
 - their exposure to third-party infrastructure or higher-risk jurisdictions creates additional financial crime risks.

Customer due diligence

- 4.18 Under [Regulation 27](#) of the MLRs, firms subject to the MLRs must apply customer due diligence (CDD) measures. Under [Regulation 33](#), firms must apply enhanced due diligence (EDD) where there is a higher risk of money laundering or terrorist financing, including where transactions are unusually complex or display unusual patterns.
- 4.19 When assessing whether a business relationship or transaction involving DeFi presents a high risk of money laundering, terrorist financing or proliferation financing, firms should consider the following non-exhaustive factors, in addition to those listed in the FCG:
- exposure to wallets, protocols or services associated with illicit activity or sanctions risk;
 - the use of privacy-enhancing technologies;
 - transaction structures involving multiple protocols, services or blockchain networks that make fund flows more difficult to understand; and
 - other indicators that may suggest attempts to obscure the origin, ownership or destination of funds.
- 4.20 Firms should ensure that they can identify, assess and manage financial crime risks when providing financial services using DeFi, including understanding the source of funds where appropriate. Firms should refer to FCG 3.2.7 and FCG 3.2.8 for further guidance on higher-risk situations.
- 4.21 Where firms identify risks, they should consider whether additional information or monitoring is necessary to understand the nature of the activity and whether it is consistent with the customer's risk profile.

Ongoing monitoring

- 4.22 As set out in FCG 3.2.5, firms should conduct ongoing monitoring on a risk-sensitive basis. Where firms provide financial services using DeFi, they should consider whether the nature of the protocols, transaction flows and blockchain activity involved requires additional monitoring to identify financial crime risks.
- 4.23 Relevant factors could include:
- interactions with newly deployed cryptoassets, tokenised assets or smart contracts;
 - indicators of fraud, including activity associated with potential rug pulls or account compromise;
 - transaction patterns that may indicate layering, obfuscation or other attempts to conceal the source or destination of funds; and
 - direct or indirect exposure to sanctioned persons, wallets, protocols or services.

Suspicious activity reporting

- 4.24 Firms should ensure they understand and comply with their legal obligations to report knowledge or suspicion of money laundering, terrorist financing or proliferation financing. The circumstances in which a report is required will depend on the applicable legislation and the facts of the case.
- 4.25 Firms should know how to draft and file a suspicious activity report (SAR), and what to report to the National Crime Agency. Firms should also understand the difference between reporting suspicions to the NCA and sanctions requirements. Based on the identified suspicious activities, firms should ensure their ongoing (transaction) monitoring approach is strengthened to reflect their latest and ongoing understanding of suspicious activities.

Travel rule

- 4.26 Firms in scope of the MLRs must comply with the requirements in Regulation 64 of the MLRs (the Travel Rule) where those requirements apply to a cryptoasset transfer.
- 4.27 Firms should assess whether their use of DeFi affects their ability to obtain, verify, transmit and retain the information required under the Travel Rule. This may be more difficult where transfers involve non-custodial wallets, multiple intermediaries or environments with differing levels of customer identification and record keeping. Nonetheless, as non-custodial wallets could pose specific illicit finance risks, and could potentially be used to avoid MLR controls, firms must mitigate the relevant risks. Under Regulation 64G of the MLRs, firms involved in a non-custodial wallet transfer may request information from their customers (whether they are an originator or beneficiary).
- 4.28 Firms should maintain procedures for dealing with missing or incomplete information (including originator and beneficiary information), assessing the associated risks and determining the appropriate treatment of the transfer. For further guidance on compliance with the Travel Rule when making transfers involving non-custodial wallets, firms should refer to the Joint Money Laundering Steering Group (JMLSG) Travel Rule guidance.

Annex 2 DeFi ecosystem

FATF's Targeted Report on Regulatory Challenges from Decentralised Finance and IOSCO's 2022 Report on Decentralized Finance describe the DeFi ecosystem as a multi-layered architecture, where each layer builds on the one below it (also called the "DeFi stack"). These layers include:

- Settlement layer – Foundational distributed-ledger infrastructure.
- Asset layer – Includes cryptoassets native to a blockchain or native to the protocols running on a blockchain.
- Protocol layer – Includes back-end smart contracts that encode financial logic, such as automated market makers (AMMs), lending/borrowing markets and liquidity pools.
- Application layer – Includes front-end interfaces, sites and smartphone apps, dashboards, applications and other tools that make the underlying protocol providing DeFi usable for non-technical users.
- Aggregation layer – Includes platforms that combine several DeFi applications in one location, enabling users to buy and sell cryptoassets or tokenised assets.

Where this guidance refers to firms providing financial services using DeFi, "DeFi" encompasses components across the DeFi ecosystem, at multiple layers of the DeFi stack.

Our approach focuses on whether a firm providing financial services using DeFi or interacting with DeFi is carrying on a regulated activity under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (including the Cryptoassets Regulations 2026), rather than where it sits on the DeFi stack.

Annex 3 Glossary

Unless linked back to an existing FCA definition or rule, terms used in this guidance consultation (GC) reflect common industry terms and are not legal terms or definitions in legislation or regulatory rules.

Term	Definition
Bridge	A protocol that connects blockchain networks to enable the transfer of assets, tokens and data between them.
Decentralised exchange (DEX)	A platform that allows users to trade crypto directly from their wallets via smart contracts, without a custodial intermediary, and which is described as decentralised.
Distributed ledger technology (DLT)	The protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions and update records in a synchronised way across a network.
Liquidity pool	A pool of cryptoassets controlled by smart contracts to support activities such as trading or lending without a traditional human counterparty.
Node operator	An individual or business that manages the servers, hardware, and software required to run a blockchain node.
Oracle	A service that supplies smart contracts with data from outside the blockchain, such as prices or information from another network.
Remote Procedure Call (RPC) node	A node allowing for external applications to communicate remotely with a blockchain.
Smart contract	Software programs deployed on a blockchain that offer functionality to run self-executing code.
Validator	A node that participates in a blockchain consensus mechanism by checking and, where applicable, proposing or attesting to blocks, according to the network rules.