

Consultation Paper

CP25/25***

Application of FCA Handbook for Regulated Cryptoasset Activities

September 2025

How to respond

We are asking for comments on Chapters 1 to 5 of this Consultation Paper (CP) by **12 November 2025** and comments on the discussion chapters 6 and 7 by **15 October 2025**.

You can send them to us using the form on our [website](#).

Or in writing to:

Crypto Policy Team
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Email:
cp25-25@fca.org.uk.

All our publications are available to download from www.fca.org.uk.

Request an alternative format

Please complete this [form](#) if you require this content in an alternative format.

Or call 0207 066 1000



Sign up for our news and publications alerts

See all our latest press releases, consultations and speeches.

Disclaimer

When we make rules, we are required to publish:

- a list of the names of respondents who made representations where those respondents consented to the publication of their names,
- an account of the representations we receive, and
- an account of how we have responded to the representations.

In your response, please indicate:

- if you consent to the publication of your name. If you are replying from an organisation, we will assume that the respondent is the organisation and will publish that name, unless you indicate that you are responding in an individual capacity (in which case, we will publish your name),
- if you wish your response to be treated as confidential. We will have regard to this indication, but may not be able to maintain confidentiality where we are subject to a legal duty to publish or disclose the information in question.

We may be required to publish or disclose information, including confidential information, such as your name and the contents of your response if required to do so by law, for example under the Freedom of Information Act 2000, or in the discharge of our functions. Please note that we will not regard a standard confidentiality statement in an email message as a request for non-disclosure.

Irrespective of whether you indicate that your response should be treated as confidential, we are obliged to publish an account of all the representations we receive when we make the rules.

Further information on about the FCA's use of personal data can be found on the FCA website at: <https://www.fca.org.uk/privacy>.

Contents

Chapter 1	Summary	Page 4
Chapter 2	High Level Standards and supervision	Page 14
Chapter 3	Senior Management Arrangements, System and Controls (SYSC) ..	Page 21
Chapter 4	Guidance on cryptoasset operational resilience.	Page 41
Chapter 5	Business standards.....	Page 55
Chapter 6	Discussion Chapter – Applying the Consumer Duty and access to the Financial Ombudsman Service to regulated cryptoasset activities.	Page 57
Chapter 7	Discussion Chapter – Conduct of Business Sourcebook and Product Intervention and Product Governance Sourcebook.	Page 67
Chapter 8	Next steps	Page 77
Annex 1	Questions in this paper	Page 78
Annex 2	Cost benefit analysis	Page 81
Annex 3	Compatibility statement.....	Page 129
Annex 4	Abbreviations used in this paper.	Page 134
Appendix 1	Draft Handbook text	

On 19 September 2025, we updated a figure in paragraph 7.23, page 71.

Chapter 1

Summary

Why we are consulting

- 1.1** In April 2025, the Treasury published a draft Statutory Instrument (SI) and Policy Note. These outlined upcoming statutory provisions to create new regulated activities for cryptoassets under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (the RAO).
- 1.2** When the final SI is made and comes into force, it will bring certain cryptoasset activities under our remit, which is currently limited to financial promotions and preventing financial crime. Cryptoasset activities that will come under our remit as a result of the SI will include issuing qualifying stablecoins, safeguarding qualifying cryptoassets and specified investment cryptoassets, operating a qualifying cryptoasset trading platform (CATP), intermediation and staking.
- 1.3** Firms and individuals conducting these new regulated activities will need to apply for authorisation before carrying out any of them by way of business in the UK.
- 1.4** This paper looks at how our rules will apply to these firms. In future, some of the firms with new cryptoasset permissions may also have Part 4A permissions for existing traditional finance products as well. In these cases, existing Handbook provisions and requirements will continue to apply to these firms.
- 1.5** The proposed new rules and guidance in our Handbook will generally apply to firms, regardless of the specific cryptoasset activities the firm undertakes. This aligns cryptoasset firms with standards expected of existing FSMA-authorised firms. The aim is to ensure cryptoasset firms have the appropriate systems, controls, processes, financial resources and people in place. These proposals will be completed by activity-specific rules which we will consult on separately later this year.
- 1.6** We are also seeking feedback on the application of the Consumer Duty (the Duty), Conduct of Business (COBS) and Product Intervention and Product Governance (PROD) Sourcebooks, Dispute Resolution (DISP 1) and access to the Financial Ombudsman Service for cryptoasset firms. We have included discussion elements on these in this paper. We will use responses to this discussion to inform subsequent proposals in future CPs (Consultation Papers) in the Crypto Roadmap.
- 1.7** The standards we are consulting on are similar to the standards we expect of all the firms we regulate. We have made changes to these to reflect the unique nature of cryptoassets, and the specific risks we have seen, to ensure we strike the right balance. The standards, if adopted, would help reduce some of the risks prevalent in the business practices in this sector. However, they do not address the underlying and inherent risks posed by cryptoassets.

1.8 We are monitoring new and established cryptoasset regulatory regimes and market trends globally, and how they are responding to risks of harm posed by different cryptoasset activities, and this has informed our proposals.

1.9 We have used our engagement with consumers and industry (both cryptoassets and traditional financial services) to inform our proposals. They also reflect feedback from the [2023 Treasury Consultation](#) and the Discussion Paper on Regulating Cryptoasset Activities ([DP25/1](#)). When developing our Policy Statement(s) we will also consider feedback from the Qualifying Stablecoin Issuance and Cryptoasset Custody CP ([CP25/14](#)) and other future relevant consultations.

FCA strategy and objectives

1.10 Our proposals reflect our statutory objectives (see pages 7-8) and our [2025-30 Strategy](#). The proposals aim to:

- **Support growth:** we want to enable cryptoasset firms to develop and innovate in a sustainable way, designing a proportionate regime that allows firms that set up in the UK to compete internationally and support the growth of the UK in the medium to long term.
- **Help consumers:** we want consumers to receive appropriate protection. We want to ensure they can stay informed and have access to products that meet their needs and offer fair value.
- **Fight crime:** our proposals aim to help cryptoasset firms act as a strong line of defence against financial crime. They should focus on designing crime out of activities involving cryptoassets. Firms should look to minimise the use of cryptoassets for fraud, money laundering, terrorist and proliferation financing or any other criminal activities.
- **Be a smarter regulator:** we are making sure our regulation is effective and proportionate.

Scope of this Paper

Consultation

1.11 Our proposals in this CP relate to the rules and guidance from the following cross-cutting Handbook areas to cryptoasset firms:

High Level Standards	PRIN Principles for Businesses (excluding the Duty) SYSC Senior Management Arrangements, Systems and Controls COCON Code of Conduct COND Threshold Conditions FIT Fit and Proper test for Employees and Senior Personnel GEN General Provisions
Business Standards	ESG Environmental, Social and Governance sourcebook
Regulatory Processes	SUP Supervision DEPP Decision Procedure and Penalties Manual
Regulatory/Registry Guides	FCG Financial Crime Guide: A firm's guide to countering financial crime risks (FCG) FCTR Financial Crime Thematic Reviews
Glossary	Relevant Glossary Terms

1.12 We are also consulting on non-Handbook guidance to support the operation of SYSC 15A on operational resilience.

Discussion

1.13 This paper also discusses the possible ways we can apply, or achieve similar outcomes to, the Consumer Duty. It discusses the conduct of business and product governance sourcebooks, as well as whether access to the Financial Ombudsman Service and the Dispute Resolution (DISP 1) rules should be extended to cryptoasset firms.

The wider context and our objectives

What we want to achieve

1.14 By applying appropriate provisions of our Handbook to cryptoasset firms, we want to ensure they will:

- Operate with integrity and transparency, helping build trust in the financial system while protecting consumers.
- Treat consumers fairly, be transparent about their products and services and effectively manage any potential conflicts of interest.

- Have operational resilience, with robust arrangements, controls and policies to prevent, respond to, and recover from operational and technical disruptions such as cyber-attacks or third-party failures.
- Identify, assess, monitor and manage risks of money laundering, terrorist and proliferation financing and other criminal activities, reducing illicit financial activities in this sector.
- Have clear accountability, promoting personal responsibility, and improving conduct in firms, by applying the Senior Managers and Certification Regime (SM&CR) regime to firms' systems and controls.

Outcomes we are seeking

1.15 We want to create a market that works well for consumers, encourages effective competition and enhances market integrity, including:

- Effective competition that delivers high quality offerings and drives innovation in the UK cryptoasset sector.
- Appropriate consumer protection for users of cryptoasset services.
- Consumers are appropriately informed of risks before investing in cryptoassets and using services.
- Cryptoassets used within our regime are not attractive for fraud, money laundering, terrorist and proliferation financing or any other criminal activities.
- The international competitiveness of the economy of the UK is supported, as well as its growth in the medium to long term, and firms are encouraged to set up in the UK to offer cryptoasset products and services.
- Well-run firms with appropriate standards and sufficient resources, subject to clear and proportionate standards which we can supervise effectively.

How our proposals link to our objectives

1.16 Our proposals are aligned with our primary strategic and operational objectives – consumer protection, market integrity, and effective competition – and advance our secondary international competitiveness and growth objective, as far as reasonably possible.

Consumer protection

1.17 We want to ensure that consumers of cryptoasset firms get an appropriate level of protection. While cryptoassets are generally high-risk and highly volatile, customers should still be protected from poor business practices.

1.18 Our proposals aim to apply similar requirements and guidance from our Handbook to cryptoasset firms as to traditional financial firms where appropriate. This includes rules on conduct (such as product design and disclosures), governance (including SM&CR), financial crime, and operational resilience. These measures are designed to reduce risks of harm from poor conduct, weak governance, financial crime and inadequate systems and controls.

1.19 In the long term, a well-regulated and competitive market will underpin sustainable growth, attract investment and position the UK as a global leader in cryptoasset services.

Market integrity

1.20 Our proposals aim to increase confidence in the UK cryptoasset market, with firms held to the same regulatory standards that apply to other FSMA-authorised firms. Ensuring that firms have the appropriate systems, controls, processes and people in place is fundamental to the trust that consumers place in firms; supporting a well-functioning and robust market.

Effective competition

1.21 Our proposals are designed to enhance consumer trust and apply appropriately robust standards. This will support consumer engagement with the market and potentially increase demand. A clear regulatory framework will provide businesses with certainty and encourage well-run firms to enter the market. This may further support effective competition and supporting innovation.

1.22 While we expect increased initial costs and some barriers to entry from the introduction of new rules in this sector, we have ensured our proposals are flexible and proportionate.

Secondary international competitiveness and growth objective

1.23 We want the UK cryptoasset market to be competitive on the global stage and for a stable and proportionate regulatory framework to play a role in fostering an innovative cryptoasset sector in the UK.

1.24 We led the development of the [IOSCO Crypto and Digital Assets Recommendations](#). These provide a baseline of regulation for cryptoassets around the world which encourages competition while guarding against a 'race to the bottom'. We consider the proposals in this CP to be aligned with international standards.

The harm we are trying to reduce and how

1.25 Where appropriate, our proposals are based on the principle of 'same risk, same regulatory outcome'. However, some risks posed by cryptoassets are due to the novel features and business models of the technology used.

1.26 Risks will remain in the cryptoasset sector even with regulation. Anyone who buys cryptoassets should be aware of the risk that they may lose all of their money, and the potential for significant volatility in most cryptoassets' value.

Poor governance and conduct

1.27 Poor governance and conduct can make it less likely that firms will act in consumers' best interest. We propose applying the existing Handbook rules and guidance on governance to cryptoasset firms, making changes where appropriate.

1.28 We also intend to implement a personal accountability regime that improves decision-making processes, improves individual conduct, and instils a firm-wide culture of regulatory compliance, for the benefit of both consumers and firms.

Financial crime, fraud and sanctions evasion

1.29 Cryptoassets appeal to criminals who exploit their permissionless and cross-border nature for illicit purposes, including fraud, money laundering, terrorist and proliferation financing and sanctions evasion. As fiat-referenced stablecoins are perceived as more stable than other cryptoassets, they have become increasingly attractive to criminals seeking to avoid the market volatility of unbacked cryptoassets.

1.30 While money laundering, terrorist financing and proliferation financing involving cryptoassets remains relatively small in absolute terms compared to traditional finance (such as cash), it is a growing concern. This has been reflected in the National Risk Assessment (NRA) for Money Laundering and Terrorist Financing 2025 by the Treasury and Home Office. This has raised the risk for money laundering for Cryptoasset Service Providers from 'Medium' to 'High' due to an increase in both criminal and legitimate use by the public, alongside the speed with which money can be moved. These concerns are largely mirrored in terrorist financing risk assessment, however the smaller increase in scale means that this risk has remained 'Medium'.

1.31 Our proposals supplement existing requirements to ensure that firms have the correct systems and controls, and adequate policies to identify, assess and manage money laundering risks and other criminal activities. This will complement the Treasury's aim to update the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) framework, in line with their response to their consultation on improving the effectiveness of the MLRs. Taken together, these measures should help further reduce the financial crime and sanctions evasion risks of cryptoassets in the UK, creating a cleaner market for consumers.

Poor operational resilience

1.32 As with traditional finance firms, a lack of operational resilience is a significant risk for cryptoasset firms.

1.33 Our proposals seek to ensure that all cryptoasset firms must meet robust operational resilience requirements, considering in particular cyber attacks, system outages and third-party supplier failure. We propose to apply SYSC 15A (along with our other operational resilience standards like SYSC 4, 7 and 8) because of the major harmful impacts of operational failures in the cryptoasset market. This will help firms to better prevent, adapt, respond to, recover and learn from operational disruptions, minimising harm to consumers and the risk to market integrity from disruption.

Interaction with our existing and broader cryptoasset regime

Interaction with other FCA discussion papers and consultation papers

1.34 There are several ongoing consultation processes which may affect the proposals in this paper. Where possible, we have highlighted these areas in their relevant chapters, alongside details on how we intend to ensure clarity and minimise duplication. However, readers are recommended to consider the other publications when they are published.

Interaction with our existing FSMA regime

1.35 We intend to apply the majority of existing rules and guidance in our Handbook to cryptoasset firms in the same way as we do to traditional finance firms, in line with our overarching principle of 'same risk, same regulatory outcome'.

1.36 We propose to expand the glossary definition of 'designated investment business' (DIB) in the Handbook to capture qualifying cryptoasset activities. DIB is an existing term defined in the Handbook's glossary which applies to a range of investment activities. Having considered and mapped across the type of activities currently captured in the DIB definition, the proposed cryptoasset activities to be introduced in legislation are similar or equivalent to the traditional finance activities that currently fall under the DIB definition. In line with the principle of 'same risk, same regulatory outcome', we propose to expand DIB to capture all cryptoasset activities. DIB also has the effect of causing many COBS provisions to apply to cryptoasset activities. However, we are not consulting on that here as COBS is dealt with in the Discussion Chapter 7.

Application to new and existing regulated firms

1.37 We propose to apply the Handbook's cross-cutting standards across the business of cryptoasset firms.

1.38 Where a firm must comply with stricter regulatory requirements based on its other authorised activities, these stricter requirements will continue to apply on the firm level whether or not the firm obtains additional permissions to conduct cryptoasset regulated activities.

1.39 Going forward, existing MLR-registered cryptoasset firms will have to seek FSMA RAO authorisations and be subject to Handbook requirements, in the same way as existing FSMA-authorised firms.

1.40 Although we are not consulting specifically on applying the CASS sourcebook in this CP, designating qualifying cryptoasset activities as DIB will lead to the application of CASS 7 for cryptoasset firms in certain instances. As highlighted in CP25/15 (a prudential regime for cryptoasset firms), firms may sometimes hold client money in connection with regulated activities involving qualifying cryptoassets held in custody. For example, where fiat currency is held for the purpose of buying qualifying cryptoassets on behalf of clients (eg on or off ramping) or when a client's qualifying cryptoasset holding changes and fiat is involved. The use of DIB will mean that the client money rules in CASS 7 apply in these instances, which was broadly supported by responses to DP23/4 (stablecoins).

Question 1: Do you agree that new cryptoasset activities defined in the SI (and as described as 'qualifying cryptoasset activities' in draft FCA Handbook rules) should fall under the category of 'designated investment business' for the purposes of applying relevant sections of the Handbook?

Our authorisations, supervision and enforcement approach

1.41 Currently, firms that provide cryptoasset services that come within the scope of the MLRs must be registered with the FCA. Cryptoasset businesses that want to market to UK consumers (ie communicate their own cryptoasset financial promotions) must also be registered with the FCA under the MLRs. The exception to this is if their financial promotions are approved by an authorised person or otherwise rely on an exemption in the Financial Promotion Order.

1.42 Under the new regime, cryptoasset firms will need to comply with the MLRs but are unlikely to need separate registration under the MLRs (subject to future Treasury legislation). Instead, they must be authorised under FSMA and will remain under ongoing FCA supervision.

1.43 To be authorised a firm must show that it satisfies, and will continue to satisfy, the minimum standards in FSMA. These are referred to as the Threshold Conditions. Our website gives more information on [applying for authorisation](#), along with details of our pre-application support service (PASS).

1.44 Our approach to supervision seeks to be proportionate, prioritising key areas of focus and firms that pose a higher risk to our objectives. We focus our engagement on areas of greatest harm and take a more flexible approach, with less intensive supervision for those firms demonstrably seeking to do the right thing. We also intend to make our areas of focus predictable so that firms have an opportunity to make positive change without the need for regulatory action. In our strategy, we have committed to streamlining how we set our supervisory priorities and sharing more insights from our supervisory work.

1.45 Our enforcement approach aims to ensure there are real and meaningful consequences for firms and individuals who do not follow our rules and who cause significant harm to consumers and markets. We consider the deterrent impact of any enforcement action and focus our efforts on achieving impactful deterrence. Our [Enforcement Information Guide](#) gives an overview of our enforcement powers, our typical process for enforcement cases and information on mediation and settlement. Our [Enforcement Guide](#) explains how we conduct a typical enforcement investigation and how we use our powers to investigate and take enforcement action. We will conduct our investigations in accordance with our policy set out in our Enforcement Guide. Further information about our enforcement approach can be found on our website.

Measuring success

1.46 We would expect to see benefits, including:

- Consumers accessing, assessing and acting on information, and a range of suppliers who compete without undue barriers.
- Increased consumer trust, with consumers accessing products and services which meet their needs.
- A reduction in cryptoassets being used to facilitate criminal activities, including fraud, money laundering, terrorist and proliferation financing to make the cryptoasset environment safer.
- The UK being a location in which cryptoasset firms choose to establish and operate from.
- Increased confidence in cryptoasset firms so that consumers have a positive experience when dealing with them, empowering them to make informed decisions. We will look to measure this through consumer research.

1.47 Alongside the above criteria, we will monitor how firms adapt to the new regime, the outcomes for consumers and other relevant factors to determine if the regime is delivering good outcomes.

Consultation with the CBA Panel and other statutory panels

1.48 We consulted the Cost Benefit Analysis (CBA) Panel in preparing the CBA included in Annex 2, in line with the requirements of [s138IA\(2\)\(a\)](#) Financial Services and Markets Act 2000 (FSMA). A summary of their main recommendations and our subsequent changes are in the 'Consultation with the FCA Cost Benefit Analysis Panel' section of the CBA.

1.49 We have also engaged with the Financial Services Consumer Panel, Practitioner Panel, and Business Practitioner Panel, and considered their input and views.

Equality and diversity considerations

1.50 We do not consider that our proposals should materially or differently 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). We know that certain demographic segments are overrepresented in cryptoasset ownership. Based on analysis from our Financial Lives Survey (2024) which is reflected in our Consumer Research series on cryptoassets (2024), cryptoasset owners are:

- Around 3 times more likely to be men.
- More likely to be younger, with 18–34-year-olds accounting for 41% of all cryptoasset owners.
- More likely to be from an ethnic minority background, which may in part be driven by the lower age profile of cryptoasset owners and greater ownership in London compared with other regions.
- More likely to have a higher-than-average household income.

1.51 While these groups are currently overrepresented in their ownership of cryptoassets, we expect all consumers who interact with cryptoassets will benefit from a regulatory regime for cryptoasset firms.

Digitally excluded customers

1.52 We do not envisage our proposals will have a direct impact on the digitally excluded, as many digitally excluded consumers do not interact with cryptoassets or the digital services needed to buy them. We also do not envisage the proposals will have a direct impact on those that use cash or lead to lower rates of using cash.

Who should read this Consultation and Discussion

1.53 Who needs to read this document:

- Firms that want to conduct regulated cryptoasset activities.
- Industry groups, law firms and trade bodies representing firms in the cryptoasset sector.
- Auditors providing services to cryptoasset firms.
- Professional advisors in the cryptoasset sector and law firms.
- Consumers and groups representing consumer interests.
- Issuers of electronic money and payment service providers.

Next steps

1.54 We welcome feedback on our proposed rules, guidance and other issues discussed in this CP and Discussion Chapters. The specific questions for feedback are in Annex 1.

1.55 The consultation period will end on 12 November 2025. We will consider the feedback received before publishing our final rules.

1.56 The discussion period will end on 15 October 2025. We will then consider the responses received before consulting on these provisions later this year.

1.57 You can send us your comments using the form on our [website](#). If you are not able to use the form, write to us at cp25-25@fca.org.uk.

1.58 In line with our [Crypto Roadmap](#), we will consult separately on proposed activity-specific rules and guidance for the cryptoasset activities outlined in [DP25/1](#) (cryptoasset activities). We will also consult separately on the admissions and disclosure and the market abuse regime for cryptoassets. We consulted on qualifying stablecoin issuance and cryptoasset custody ([CP25/14](#)) and the prudential regime for cryptoasset firms ([CP25/15](#)) in May 2025, and will consult on the remaining prudential items as set out in the Crypto Roadmap. Following consideration of responses to these consultations, our final rules and guidance will then be set out in Policy Statement(s).

1.59 We recover our costs from the firms we regulate. We intend to consult on our proposals for charging cryptoasset firms as part of our annual consultation on fees policy, which is due for publication in November 2025.

Chapter 2

High Level Standards and supervision

Applying High Level Standards to cryptoasset firms

2.1 The FCA Handbook sets out rules and other provisions made under our powers in the Financial Services and Markets Act 2000 (FSMA). The Handbook includes 'High-Level Standards' – core principles that define the fundamental obligations that apply to all FCA authorised firms. We propose to apply these standards to cryptoasset firms in addition to the specific rules set out in later chapters and other consultation papers set out in our [Crypto Roadmap](#). They will give firms a clear statement of the standards of behaviour we expect and help address the harms identified in the market. This chapter gives more information on these standards. We will also set out guidance for our supervision of firms.

2.2 In this chapter we set out our proposals on applying:

Sourcebook	Description
COND Threshold Conditions	These are the minimum conditions for which we are responsible, a firm is required to satisfy, and continue to satisfy, to be given and to keep its permissions. We provide guidance on these conditions in COND.
PRIN Principles for Businesses	These are a general statement of the fundamental obligations that firms must always comply with.
GEN General Provisions	This section sets out some of the requirements that apply to all firms, including statutory disclosure statements and use of the FCA name or logo.
SUP Supervision	SUP provides guidance for our supervision of firms to ensure they meet regulatory standards.

Stakeholders feedback

2.3 In developing our proposals, we have considered the feedback to our published discussion/consultation papers. For example, the majority of industry responses (c. 96%) to our [DP23/4](#) (stablecoins) supported applying FCA High Level Standards as part of the new regime we propose to introduce.

Threshold Conditions

2.4 Threshold Conditions (COND) are the minimum conditions a firm is required to satisfy, and continue to satisfy, to be given and keep its permissions. As set out in FSMA, firms must comply with COND to be authorised.

2.5 We propose to apply COND to cryptoasset firms. These firms should refer to COND and the guide on Threshold Conditions to understand them in more detail. As these are set out in FSMA we are not consulting on the Threshold Conditions themselves, but on applying COND to cryptoasset firms.

Principles for Businesses

Overview of the current framework

2.6 The Principles for Businesses (PRIN) set out in the PRIN chapter of the Handbook apply in whole or in part to every authorised firm. They are a general statement of the fundamental obligations of firms and the other persons to whom they apply under the regulatory system.

Applying PRIN to cryptoasset firms

2.7 We are consulting on applying PRIN to cryptoasset firms, apart from the exceptions discussed below. This is a proportionate response to the specific risks in the crypto sector. Our aim is to ensure these firms meet robust regulatory standards and effectively manage cryptoasset-related risks. We believe the framework used for traditional finance firms sufficiently addresses these risks and so should also apply to cryptoasset firms.

2.8 In line with the approach for existing FSMA-authorised firms that only service institutional clients or professional clients, we will disapply relevant parts of PRIN for business with eligible counterparties (ECPs). We are not looking to make any changes to provisions relating to COBS 3 Client Categorisation to do this. We will be separately consulting on proposed changes to COBS 3 in the near future across all sectors, including cryptoassets.

2.9 Several of the Principles impose requirements on firms for their customers. For cryptoasset specified activities, we propose the definition of customer and client in PRIN will include a holder of a qualifying stablecoin.

The Principles

1 Integrity	A <u>firm</u> must conduct its business with integrity.
2 Skill, care and diligence	A <u>firm</u> must conduct its business with due skill, care and diligence.
3 Management and control	A <u>firm</u> must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
4 Financial prudence	A <u>firm</u> must maintain adequate financial resources.
5 Market conduct	A <u>firm</u> must observe proper standards of market conduct.
6 Customers' interests	A <u>firm</u> must pay due regard to the interests of its <u>customers</u> and treat them fairly.
7 Communications with clients	A <u>firm</u> must pay due regard to the information needs of its <u>clients</u> , and communicate information to them in a way which is clear, fair and not misleading.
8 Conflicts of interest	A <u>firm</u> must manage conflicts of interest fairly, both between itself and its <u>customers</u> and between a <u>customer</u> and another client.
9 Customers: relationships of trust	A <u>firm</u> must take reasonable care to ensure the suitability of its advice and discretionary decisions for any <u>customer</u> who is entitled to rely upon its judgment.
10 Clients' assets	A <u>firm</u> must arrange adequate protection for <u>clients' assets</u> when it is responsible for them.
11 Relations with regulators	A <u>firm</u> must deal with its regulators in an open and cooperative way, and must disclose to the <u>FCA</u> appropriately anything relating to the <u>firm</u> of which that regulator would reasonably expect notice.

Disapplying specific Principles

2.10 We propose not to apply Principles 1, 2, 6 and 9 to transactions entered into on a CATP by its members. This is similar to the position of transactions on multi-lateral trading venues in traditional finance, and recognises the role of platform operators in monitoring and overseeing compliance with the CATPs own trading rules, when it comes to transactions on their own platforms. We also propose that CATPs owe obligations to retail investors under PRIN, where applicable. Our proposal is designed to protect retail customers who have direct market access to CATPs in cryptoasset markets, which is typically not the case in other traditional finance sectors where retail customers largely transact through intermediaries.

Disapplication of Principles to transactions entered into on a CATP by its members

Principles	1 Integrity 2 Skill, care and diligence 6 Customers' interests 9 Customers: relationships of trust
-------------------	---

2.11 Similarly, Principles 6 and 9 will not apply when a firm provides the service of operating a CATP for professional clients. This is consistent with the case of trading venues in traditional finance and the absence of a regulated activity of advising on qualifying cryptoassets.

Disapplication of Principles to firms which provides the service of operating a CATP for professional clients

Principles	6 Customers' interests 9 Customers: relationships of trust
-------------------	---

The Consumer Duty

2.12 Principle 12, PRIN 2A and PRIN 3 include our rules and guidance for the Duty. We discuss our approach to the Duty in more detail in Chapter 6. As we are not consulting on the application of the Duty at this time, we are not proposing to apply Principle 12 to any regulated cryptoasset activities in this CP. We will consult on our approach to the Duty in a later consultation paper.

General Provisions

2.13 The General Provisions (GEN) contain rules covering administrative duties that apply to the firms we regulate. These include rules on how firms should refer to their regulatory status, interpret rules in our Handbook and behave in an emergency. The intention of these rules is to make sure consumers are not misled, that all firms operate on a level playing field and that firms are transparent about their regulatory status. We propose to apply GEN to cryptoasset firms.

2.14 GEN contains:

- The ban on firms claiming or implying that we have endorsed their business.
- Steps firms should take in situations when they cannot comply with our rules in an emergency.
- Guidance on how to interpret our Handbook of rules and guidance.
- Rules on how firms authorised by us must describe their regulatory status: 'status disclosure'.
- Restrictions on using our name and our logo.
- The ban on taking out indemnity insurance against the risk of having to pay financial penalties.
- The ban on firms charging a consumer more than a basic rate to call its telephone line where it has a contract with the consumer.

2.15 This is not a complete list and we expect cryptoasset firms to familiarise themselves with GEN more broadly.

Question 2: Do you agree with our proposal for applying High Level Standards to cryptoasset firms in a similar way they apply to traditional finance?

Supervision Manual

Overview of the current framework

2.16 Supervision is the oversight of firms and individuals to reduce actual and potential harm to consumers and markets. The core elements of our supervisory approach are set out in SUP. SUP outlines how we supervise firms and individuals to ensure they meet regulatory standards. It includes rules and guidance on:

- Information gathering by the FCA.
- Skilled person reviews.
- Auditors.
- Permissions and variations.
- Notification obligations.

2.17 Our website has further information on our [approach to supervision and supervision](#).

Applying SUP to cryptoasset firms

2.18 We propose:

- Extending and applying the relevant sections of SUP to cryptoasset firms.
- Requiring cryptoasset firms to notify us of significant changes in their business.

2.19 The table below summarises the key sections of SUP that we propose applying to cryptoasset firms in line with other firms that we regulate. We will set out our proposals on [SUP 16 Reporting Requirements](#) in future consultation papers.

Handbook reference	Key rule and references
SUP 2 Information gathering by the FCA or PRA on its own initiative	We can gather information in multiple ways: through meetings with firms, visits, information requests or mystery shopping. SUP 2 also explains the limitations of our powers when accessing protected items or those with specific confidentiality. A firm must also take reasonable steps to ensure that outsourced suppliers are open and co-operative with our information-gathering work.

Handbook reference	Key rule and references
SUP 3 Auditors	<p>Auditors act as an important source of information for us in our supervision of a firm's compliance with applicable requirements and standards. For firms required to appoint auditors, this chapter lays out the auditor's role, which can include reporting on metrics such as a firm's compliance with the client asset (CASS) rules. Such CASS audits enable oversight and assurance of a firm's systems and controls to determine the effectiveness of client asset protection.</p> <p>In DP23/4 (stablecoins) we proposed requiring both stablecoin issuers and cryptoasset custodians to undertake and provide an annual CASS audit, conducted by an independent external auditor. Respondents were in favour of this approach and, as flagged in CP25/14 (stablecoin issuance and cryptoasset custody), we are proceeding with our proposal to require a CASS specific annual audit for both stablecoin issuers and cryptoasset custodians.</p>
SUP 5 Reports by skilled persons	<p>We may appoint or require a skilled person to be appointed under section 166 or section 166A of FSMA to provide us with a report on specific areas of concern. If a firm appoints a skilled person, they must co-operate with us and waive any duty of confidentiality.</p>
SUP 6 Applications to vary and cancel Part 4A permission and to impose, vary or cancel requirements	<p>Explains:</p> <ul style="list-style-type: none"> • How a firm might apply to vary or cancel its permissions. • How a firm can apply to have a new requirement imposed on it or to vary or cancel a requirement. • How we will assess such applications.
SUP 7 Individual requirements	<p>We can vary a firm's permission to carry out a regulated activity, and set individual requirements and limitations on our own initiative, ie we will take action without a request or application from the firm.</p>
SUP 8 Waiver and modification of rules	<p>We can waive or modify rules for firms, if they have applied for or consented to those changes. This explains the procedure firms and the FCA must follow to do this.</p>
SUP 9 Individual guidance	<p>We can give individual guidance to a firm. This chapter sets out the procedure for firms to get this guidance.</p>
SUP 15 Notifications to the FCA	<p>Firms must notify us either orally, in writing, or using a form (depending on the notification) about significant changes in its business.</p>

Notification of significant changes in business (SUP 15)

2.20 We propose applying our notification requirements to cryptoasset firms. This means that firms will have to notify us when there is a significant change in their business. The table below sets out each notification requirement.

SUP provision number	Notification reason	Notification method/timing
15.3.1R	Matters having a serious regulatory impact eg failure to satisfy a Threshold Condition or any matter affecting the firm's ability to provide adequate provision of services which could result in serious detriment to the consumer.	Using the <u>Notification Form</u> , or if appropriate, <u>telephone</u> , as soon as the firm is aware that an event has or may have occurred or that it might occur in the future.
15.3.8G (Principle 11) 15.3.8G subject to further consultation, see CP25/22	Anything relating to the firm of which we would reasonably expect notice, such as business restructuring or significant failure in systems or controls.	Orally or <u>in writing</u> within a time period depending on the event, but before making any internal or external commitments.
15.3.11R	Significant breach of a rule or requirements in or under FSMA or the Consumer Credit Act 1974.	Using the <u>Notification Form</u> as soon as the firm is aware, or has information which reasonably suggests, that such an event has, may have occurred or might occur in the foreseeable future.
15.3.15R	Civil, criminal or disciplinary proceedings brought against the firm.	Immediately.
15.3.17R	A significant event involving fraud, errors or other irregularities.	Immediately.
15.3.21R	Event related to insolvency, bankruptcy and winding up.	Immediately.
15.3.32R	Significant infringement of any applicable competition law.	Immediately on awareness or information reasonably suggesting infringement using <u>Notification Form</u> .
15.5.1R – 15.5.6R	Change in name, address and telephone number.	Reasonable advance notice using the <u>Notification Form</u> .

2.21 All the data that should be included in notifications can be given in the formats set out in SUP 15 Annex 4 and using the methods set out in SUP 15 Annex 4.

Question 3: Do you agree with our proposed application of the existing SUP rules (except SUP 16) to cryptoasset firms?

Chapter 3

Senior Management Arrangements, System and Controls (SYSC)

Applying SYSC and related standards to cryptoasset firms

3.1 This chapter outlines our proposals for applying the **SYSC sourcebook** to **cryptoasset firms**, setting standards for governance, systems, controls, whistleblowing, and conflicts of interest. It also covers the proposed application of related regulatory frameworks, including:

- COCON (Code of Conduct)
- FIT (Fit and Proper Test)
- SUP 10C (Senior Managers and Certification Regime)
- FCG & FCTR (Financial Crime guidance and reviews)

3.2 SYSC ensures senior managers take practical responsibility for firm arrangements and risk management, creating a consistent framework across authorised firms. Compliance helps firms assess and mitigate risks to consumers and markets.

3.3 These proposals reflect feedback from DP23/4 (stablecoins) and DP25/1 (cryptoasset activities), which explored governance, operational resilience, and broader firm standards. We discuss this feedback in the sections that follow.

Overall approach

3.4 We propose applying SYSC and related sourcebooks (COCON, FIT, SUP 10C, FCG, FCTR) to cryptoasset firms, in a similar way to how they apply to most FSMA-authorised firms. These standards will be proportionate to the risks posed, with certain areas such as operational resilience (eg SYSC 15A) applied in full to all crypto firms, given the sector's reliance on technical infrastructure.

3.5 Cryptoasset firms will generally be classified as 'other firms' under SYSC, like consumer credit firms, rather than 'common platform firms' (eg banks, investment firms), which face more complex and stringent requirements. We believe cryptoasset firms do not typically pose the same level of systemic risk.

3.6 To align crypto regulation with traditional finance, we propose expanding the definition of Designated Investment Business (DIB) to include cryptoasset activities. This ensures comparable consumer protections and applies relevant SYSC rules, such as requiring a Compliance Oversight Function (SMF16) under SYSC 6.1.4A.

3.7 Firms conducting multiple regulated activities will follow the SYSC rules which apply to each activity. For example, a cryptoasset firm with permissions that qualify it as a common platform firm would need to meet those higher standards across all its regulated activities.

3.8 Finally, we are updating the SYSC application table to reflect how these provisions will apply to cryptoasset firms.

General standards and governance

Overview of the current framework

3.9 Our general standards and governance requirements are high level. They range from skills, knowledge and expertise requirements for employees, agents and other relevant persons (SYSC 5), compliance and internal audit requirements (SYSC 6), record-keeping (SYSC 9), conflicts of interest (SYSC 10), whistleblowing (SYSC 18) to training for employees (TC). These requirements are designed to be proportionate to the level of risk that firms and their activities can pose, with more robust requirements for large and systemically important firms.

Handbook reference	Summary of areas and rationale
SYSC 1 and 4	These cover how SYSC applies to different types of firms and outline general organisational requirements for firms.
SYSC 5	This covers skills, knowledge, and expertise and sets out guidance to supplement this high-level requirement, ensuring firms employ the right personnel for the responsibilities allocated to them.
SYSC 6 and 7	These cover general compliance and risk control requirements, ensuring that firms have adequate policies and procedures to ensure compliance with our rules and guidance.
SYSC 9	This places record-keeping obligations on firms, ensuring that they maintain orderly records so we can monitor the firm's regulatory compliance.
SYSC 10	This sets out how firms ought to manage conflicts of interest to reduce the risk of harm to their customers.
SYSC 18	This sets out our expectations with respect to how firms handle whistleblowers and provides best practice guidance for appropriate arrangements.
Training and Competence (TC) sourcebook	This provides standards for firms when assessing employees as competent to carry out activities listed under TC. This allows us to supplement the guidance in SYSC 5 with more prescriptive requirements for certain activities which can pose a higher risk to a firm's customers.

Stakeholder feedback

3.10 In developing our proposals, we have considered feedback to our various published discussion and consultation papers. The majority of industry responses (~ 71%) to DP23/4 (stablecoins) recognised the importance of having robust governance requirements and broadly supported applying the high-level systems and controls requirements in SYSC, ensuring that firms have transparent organisational structures and proper internal controls.

Vulnerabilities and risks in the sector

3.11 Unless previously authorised for other regulated activities, cryptoasset firms will not have been subject to a regulatory regime under FSMA. While the basis of our standards often reflects good business practice, this means they may not have appropriate policies and procedures to assess the risks they pose to consumers and broader financial markets. For example, to evidence their compliance with their regulatory obligations, firms should have robust record-keeping policies to maintain records of customer relationships and key decisions. Firms should also maintain policies for addressing conflicts of interest and handling whistleblowers appropriately. Implementing governance changes such as these should help cryptoasset firms build up a strong compliance culture so they manage the risks to customers without requiring regulatory intervention.

3.12 Given the lack of previous regulation for cryptoasset firms, there may also be a greater risk of undiscovered and unresolved misconduct within firms. The whistleblowing best practice in SYSC 18 encourages firms to implement robust procedures to ensure they handle whistleblowing disclosures appropriately, so that whistleblowing can contribute to reducing the risks cryptoasset firms may pose to consumers and broader financial markets.

Summary of proposals

3.13 We propose to apply SYSC 1, 4 – 7, 9 – 10 and 18 relating to 'governance' to cryptoasset firms. SYSC 8 is dealt with separately in the Operational Resilience section of this chapter. Applying these SYSC chapters aims to ensure cryptoasset firms build up a robust governance and compliance framework, improving their compliance across the new cryptoasset regime, and ensuring they identify problems and take action to reduce the risks they pose to consumers and the broader market.

3.14 We recognise that SYSC 10 contains general, firm-wide standards and expectations for managing conflicts of interest. Business models in the cryptoasset market pose specific conflicts of interest risk, for example as a result of vertical integration. We intend to consult on requirements to handle specific conflicts of interest risk in our future CP, which will set out how we intend to regulate specific cryptoasset activities.

3.15 Towards the end of 2025, we intend to consult on changes to the SYSC 10 sourcebook on conflicts of interest to simplify how it applies across different types of firms. We are consulting in this CP on SYSC 10 as it currently stands, however cryptoasset firms should consider the upcoming consultation alongside any other future consultations and policy statements on SYSC 10 which will be applicable to cryptoasset firms.

3.16 As for our Training and Competence Sourcebook, in FS25/2 (feedback statement on FCA requirements), we proposed exploring alternative options for the Training and Competence (TC) requirements to help simplify our requirements on firms.

3.17 As a result, we plan to consult on applying TC to cryptoasset firms at a later date but before we publish our Policy Statements on the final cryptoasset rules. Therefore, the consultation question below does not cover the proposed application of TC to cryptoasset firms.

Question 4: **Do you agree with our proposal to require cryptoasset firms to follow the existing requirements in SYSC 1, 4 – 7, 9 – 10, and 18 in a similar way to existing FCA-regulated firms (or existing DIBs)?**

Senior Managers & Certification Regime (SM&CR)

Overview of the current framework

3.18 The Senior Managers & Certification Regime (SM&CR) aims to create clear accountability, promote personal responsibility, and improve firms' conduct. In July 2025, we published CP25/21 (SM&CR), alongside parallel consultation papers published by the Treasury and the Bank of England, which proposed streamlining the SM&CR to boost competitiveness.

Senior Managers Regime	SYSC and SUP10C cover the Senior Managers Regime. Senior Managers hold one or more roles designated as Senior Management Functions (SMFs). The individuals holding these roles are a firm's most senior individuals. These include executive roles, such as chief executives and finance directors, as well as some oversight roles, such as chairs of boards and their sub-committees and senior independent directors.
Certification Regime	SYSC 27 covers functions at a firm that are not SMFs and that have a material impact on risks to customers and the risk profile of the firm.
Conduct Rules	The COCON sourcebook sets standards of conduct for all professional employees of FSMA-authorised firms. There are additional rules for Senior Managers.

3.19 The current requirements under the SM&CR differ depending on the size and complexity of the FSMA-authorised firm. We classify solo-regulated firms as Limited, Core or Enhanced. The classification criteria are based on the activities the firm is authorised to carry out and conditions set out in [our Handbook](#), for example its total Assets Under Management or value of safe custody assets it holds.

3.20 It is important that cryptoasset firms implement robust personal accountability frameworks for senior personnel, just as other FSMA-authorised firms are required to. This will help reduce harm to consumers and strengthen market integrity by creating a system that enables firms and regulators to hold people to account for their conduct and competence when things go wrong.

Stakeholder feedback

3.21 We considered feedback provided in response to our various discussion and consultation papers. In particular, in [DP23/4 \(stablecoins\)](#) we discussed applying the existing SM&CR to stablecoin issuers and cryptoasset custodians. The majority of respondents were supportive, with some suggesting we should consider additional SMFs, additional criteria for the 'enhanced category' and additional certification functions to reflect the distinct business models of stablecoins issuers and cryptoasset custodians.

3.22 The existing SM&CR is designed so the SMFs, categorisation criteria and certification functions are not sector specific. These elements of the regime should remain relevant and applicable across different business models within financial services, while also remaining technologically agnostic (unbiased towards any specific technology).

3.23 We are proposing that cryptoasset firms should follow the existing classification approach to be consistent with our current approach to SM&CR.

3.24 The SM&CR Guide for solo-regulated firms clarifies that the 'Enhanced' criteria is designed to capture only 'a small proportion of solo-regulated firms'. Among existing FCA-regulated firms, this proportion tends to be around 1% of firms. We have reviewed the nature and profile of firms currently captured in this category and compared that with the cryptoasset sector. We have judged that these classification criteria remain valid, although we recognise Handbook changes will need to be made to SYSC 23 and SUP16 to allow the appropriate cryptoasset firms to qualify.

3.25 We also considered responses to [DP23/3 \(SM&CR review\)](#) in developing our proposals for applying SM&CR to cryptoasset firms. Responses to this DP showed wide support for the SM&CR and its aims, a general agreement that the regime is meeting its objectives and is of considerable value to firms and to UK financial services in general. In particular, most feedback suggested that the existing suite of SMFs is appropriate and fit for purpose.

3.26 Several respondents said there have been too few enforcement outcomes against individuals under the SM&CR. They were concerned that the threat would become a waning deterrent, which would weaken individual accountability and hinder the SM&CR's effectiveness.

3.27 We agree that the Senior Managers Regime in its current form is useful for instilling a culture of personal accountability and agree that action against individual SMFs is a valuable deterrent against poor conduct and decision making. The Senior Managers Regime remains a valuable tool for Authorisations to assess culture at the gateway, as well as for Supervision to maintain a culture of personal accountability in firms.

Vulnerabilities and risks in the sector

3.28 Applying the SM&CR to cryptoasset firms will help us manage the particular vulnerabilities and risks we have observed. Current market practices and recent firm incidents suggest that senior individuals at cryptoasset firms have often failed to maintain a clear and appropriate apportionment of responsibilities. Responsibilities were often overconcentrated in the hands of a few key individuals who were not constructively challenged by other members of senior management. This resulted in a failure to properly identify and assess the risks of key decisions.

3.29 In the case of the highly publicised bankruptcy of the cryptoasset exchange FTX, there was a lack of independent governance between the exchange and Alameda, a hedge fund also controlled by FTX's founder and some members of senior management. This had not been properly disclosed to consumers and investors, and created a significant conflict of interest, thereby failing to protect FTX's customers' funds.

3.30 This incident highlights the need for clear and appropriate apportionment of responsibilities and robust governance standards for cryptoasset firms, comparable to those applied in traditional financial services.

Summary of proposals

3.31 We propose to apply all the existing elements and rules of SM&CR to cryptoasset firms, in line with the current approach for authorised firms.

3.32 This approach also involves applying all relevant senior management functions, certification functions, prescribed responsibilities and conduct rules. In the table below we set out the Handbook areas that we propose to apply to all cryptoasset firms.

Handbook reference	Title
SYSC 22	Getting, giving and receiving references
SYSC 23	Introduction and firm classification
SYSC 24	Allocation of prescribed responsibilities
SYSC 25	Management responsibilities map & handover procedures and manual
SYSC 26	Overall and local responsibilities
SYSC 27	Certification Regime
SUP 10C	Requirements on SMF Managers
SUP 15.11	Notification of COCON breaches and disciplinary action
COCON	Conduct rules for firm staff
FIT	Fit and proper test for employees and senior personnel

3.33 Both our SM&CR Review and the Treasury's consultation on legislative changes are ongoing. These proposals, including the potential replacement of the Certification Regime with something more streamlined and FCA rule-based, affect all authorised firms – including cryptoasset firms once authorised – and may influence how firms respond to and implement our proposals. As the SM&CR Review and the Treasury's legislative proposals are still under consultation, we are proposing to apply the current SM&CR to cryptoasset firms for now. Firms should review all SM&CR related consultations, as final changes will be reflected in future policy updates. We will consider introducing a 'modification by consent' approach where appropriate, to enable us to temporarily waive any Handbook requirements that we consider likely to be shortly rescinded. Information on this can be found on our website.

3.34 We will continue to work closely with cryptoasset firms during the implementation of the SM&CR once our final policy statement is published and will help firms prepare for the regime to go live. This will mean helping firms when applying for authorisation to understand which elements of the SM&CR they will be expected to implement. As noted above, we continue to believe it is important that SMFs are in place for cryptoasset firms, and will expect firms to comply with SMF requirements even if we have not yet finalised other elements of SM&CR.

Applying our Senior Managers & Certification Regime (SM&CR) framework to cryptoasset firms

3.35 Our policy intention is to apply SM&CR to all firms carrying out cryptoasset activities (ie those activities defined in the Treasury's draft SI and Policy Note). However, we have highlighted particular areas of SM&CR that cryptoasset firms should consider when applying the regime to their business. We would particularly welcome responses from firms on these areas.

Proposed approach to SM&CR tiering

3.36 Our SM&CR Handbook rules and guidance apply differently to solo-regulated firms depending on which SM&CR firm tier they sit in (ie Limited, Core or Enhanced); the aim is to ensure the regime applies proportionately given the size and complexity of the firm. Cryptoasset firms should consider which category they will likely fall into when applying for authorisation, as it will determine the requirements they must comply with.

3.37 As mentioned above, we are proposing to apply the same criteria that apply to existing FCA-regulated firms. To ensure cryptoasset firms can be captured within the 'Enhanced' criteria where appropriate, we will introduce cryptoasset-specific regulatory reporting requirements within existing or new returns, this may also include further amendments to other areas of our Handbook. We will propose these Handbook changes, alongside wider cryptoasset firm reporting requirements, in a future CP. However, firms should acknowledge the approach set out in this CP and provide feedback.

Classification	Limited scope	Core	Enhanced
Criteria	We anticipate that no cryptoasset firms will be 'Limited Scope' at the gateway. Firms are only considered to fall within this category if their principal purpose is to carry on activities other than regulated activities.	Most cryptoasset firms will be in this category.	Around 1% of all authorised firms are Enhanced. These are typically larger, more systemic firms which meet the criteria we will set out. Firms can also choose to 'opt up' to become Enhanced.

3.38 The qualification criteria and thresholds we currently use to classify all solo-regulated firms would apply to cryptoasset firms. SYSC 23 in our Handbook provides a flow diagram that firms can use to work out what SMR requirements they will have to comply with. We propose applying this table to cryptoasset firms, with necessary changes to account for the different reporting requirements for cryptoasset firms and how specific cryptoasset firms are captured in our Handbook.

3.39 There are currently 6 criteria for determining whether a firm falls into the 'Enhanced' category (capturing around 1% of solo-regulated firms). As noted above, we will use a future CP to set out how we will categorise cryptoasset firms as 'Enhanced' under SM&CR and the regulatory reports they will need to complete. We are proposing that cryptoasset firms could rely on the following criteria with relevant amendments:

- a.** CASS Large firm – firms holding significant balances of client assets, currently in excess of £1bn of client money and/or £100bn as safe custody assets. While authorised cryptoasset firms will not be considered CASS Large by virtue of CASS 1A not applying to them, we are considering introducing a new criterion within SYSC 23 that resembles the metrics for qualifying as 'CASS Large' that can apply to cryptoasset firms. This could mean that cryptoasset custodian firms holding a value between £1bn and £100bn in qualifying cryptoassets on behalf of their clients will be considered 'Enhanced' for the purposes of SM&CR. We are seeking responses on where, within the range of £1bn-£100bn, the Enhanced threshold should be set for cryptoasset custodians. We want to maintain consistency with the approach taken for other authorised firms and capture a similar proportion of around 1% of firms in the market. We will be proposing new regulatory reporting returns for cryptoasset firms in a future CP, including data elements submitted via these returns, such as the firm's total qualifying cryptoassets held in custody. This will form the basis of whether a firm qualifies as Enhanced.
- b.** A firm with Assets Under Management (AUM) of £50bn or more calculated as a three-year rolling average (we are proposing in [CP25/21 \(SM&CR\)](#) to increase this threshold to £65bn). We note that the existing criteria to be captured as Enhanced based on AUM would not capture cryptoasset firms without necessary changes, particularly to account for the backing assets of qualifying stablecoins. Therefore, we will propose introducing new regulatory reporting rules so that stablecoin issuers could be classed as 'Enhanced' via an adjusted financial qualification test that closely replicates the existing metrics set out in FSA038. This means the management of stablecoin backing assets will fall within the current 'Enhanced' criteria of AUM.
- c.** Opt-up – firms can choose to opt up from Core to Enhanced.

3.40 Regardless of classification under the SM&CR all cryptoasset firms will be considered a DIB firm as noted in Chapter 1. This means cryptoasset firms will be required, as with all DIB firms, to have a Compliance Oversight Function (SMF16). The details of this requirement are in [SYSC 6.1.4R](#). Having an individual at the firm who is personally accountable and responsible for the firm's compliance policies, procedures and controls, means compliance is more likely to be prioritised at a senior level and not subordinated to business priorities. It helps ensure that the compliance function as a whole meets its responsibilities properly and independently.

Requirements specific to SM&CR Core firms

3.41 Cryptoasset firms that are categorised as Core SM&CR will be required to allocate up to 6 Senior Management Functions (SMF1, SMF3, SMF27, SMF9, SMF16 and SMF17), depending on whether the SMFs are relevant to the firm, and 5 Prescribed Responsibilities (PRs), as with all Core FCA-regulated firms. PRs are specific responsibilities defined in the FCA Handbook and PRA Rulebook that a firm must allocate among its SMFs. The details of these functions and responsibilities can be found in our Handbook or on pages 18 and 19 of the [SM&CR Guide for solo-regulated firms](#).

3.42 We do not propose to introduce any SMFs or PRs specifically for SM&CR Core cryptoasset firms. The core principles and functions of the SM&CR are intended to be relevant across financial services business models generally. While most of the PRs apply to all Core firms, PR(Z); 'Responsibility for the firm's compliance with CASS' will only be relevant to stablecoin issuance firms and cryptoasset custodian firms. In the case of a stablecoin issuers, this individual would be accountable for overseeing the backing asset pool, and for a cryptoasset custodian, their responsibility would include the operation and oversight of CASS compliance, review of processes and controls and overseeing third-party provider arrangements. Cryptoasset firms should also read this CP in conjunction with [CP25/14](#) (stablecoin issuance and crypto custody) to better understand their obligations relating to the custody of qualifying cryptoassets.

Requirements specific to SM&CR Enhanced firms

3.43 Cryptoasset firms categorised as Enhanced SM&CR will be required to allocate 11 additional Senior Management Functions (SMFs 2, 4, 5, 7, 10, 11, 12, 13, 14, 18 and 24), where those SMFs are relevant, on top of those also required for Core firms. They will be further required to allocate 7 additional PRs, as with all Enhanced FSMA-authorised firms. The details of these functions and responsibilities can be found in our Handbook or on pages 23-25 of the [SM&CR Guide for solo-regulated firms](#).

3.44 We do not propose to add any sector-specific SMFs for cryptoasset firms. We considered introducing, for example, a PR for maintaining the operational resilience of the firm's underlying blockchain technology. However, we concluded that existing Prescribed Responsibilities are sufficient to ensure personal accountability for operational failings. This is consistent with the intention behind the SM&CR; that its functions and responsibilities remain broad enough to be relevant across financial sectors.

3.45 Separately, some dual-regulated firms are subject to requirements in SYSC 25 and SYSC 26 of our handbook. We anticipate that there may be instances where firms who are dual-regulated for the purpose of carrying out other activities will also seek authorisation for the carrying out of cryptoasset activities (as defined in [HMT's Draft SI and Policy Note](#)). For example, a dual-regulated firm that meets the definition of a 'UK SM&CR Banking Firm', because of its Part 4A permission for accepting deposits, could in the future decide to seek authorisation for the activity 'dealing in cryptoassets as agent'. In such cases, firms will continue to be required to comply with the applicable requirements for dual-regulated firms. This should not be onerous for firms, as they will already be accustomed to these elements of SM&CR as a result of their other businesses being dual regulated.

3.46 As required for all Enhanced SM&CR firms, we propose Enhanced cryptoasset firms be required to have, maintain and submit to us a Management Responsibilities Map to clarify their organisational structure by outlining their governance and management arrangements. This will allow both the firm and the FCA to understand the firm's structure, reporting lines, and how Senior Manager Functions (SMFs) and prescribed responsibilities are allocated, enabling individuals to understand what they are personally accountable for, and enabling the FCA to hold the correct person to account. The details of this requirement can be found in SYSC 25 of our Handbook, or in the SM&CR Guide for solo-regulated firms.

Certification regime

3.47 To understand which Certified Functions will be relevant to cryptoasset firms' business models, and so which individuals within their firm they will be required to certify, they should review SYSC 27 of our Handbook. This provides a comprehensive list and description of the Certified Functions. Below are some elements of the regime that cryptoasset firms should consider in particular.

3.48 Firms dealing in cryptoassets as agent, and/or firms arranging (bringing about) deals in cryptoassets, will be required to certify the relevant employees carrying out these activities under the 'client dealing' function. We propose to add the latter activity to the 'activities covered by the client-dealing FCA certification function' table in SYSC 27.8.19. We believe this approach is consistent with other qualifying firms carrying out similar investment activities.

3.49 We are also amending the definition of proprietary trading so that the proprietary trading certification function covers dealing in cryptoassets as principal and issuing qualifying stablecoin in the United Kingdom. We believe this approach is consistent with the treatment of other qualifying firms carrying out proprietary trading.

3.50 Cryptoasset custodian and stablecoin issuance firms will not, under our proposals, be able to certify individuals under the [CASS oversight FCA certification function](#) in SYSC 27.8.1R. This is because CASS 1A.3, which allows firms to allocate the function in CASS 1.A.3.1AR to someone who is not a SMF manager (provided that they do hold the CASS oversight FCA certification function) will not be applicable to authorised cryptoasset firms.

3.51 We will use our future CPs to set out proposals for whether cryptoasset firms will be subject to the Algorithmic Trading Certification Function when we have consulted on other proposals on the use of algorithms for trading qualifying cryptoassets.

The Conduct Rules

3.52 This regime sets out standards of individual behaviour for employees in financial services. It is relevant to all firms, and we are proposing that the regime also be applied to cryptoasset firms in the same way.

3.53 Individuals holding SMFs at cryptoasset firms should refer to and comply with the 4 additional senior manager conduct rules in COCON 2.2.

3.54 We propose that cryptoasset firms are required, as with all authorised firms, to notify the FCA when an individual has breached the Conduct Rules and has been subject to disciplinary action as a result. The details of this requirement can be found in the SUP15.11 in the SUP sourcebook of our Handbook.

FIT: Fitness and Propriety guidance

3.55 This provides guidance for how firms should demonstrate that they are making regular, thorough and consistent assessments of the fitness and propriety of SMFs and Certification Staff. FIT sets out the main elements firms should consider when assessing an employee's fitness and propriety. These are general principles that do not require sector-specific guidance:

- Honesty, integrity, and reputation
- Competence and capability
- Financial soundness

3.56 We propose that cryptoasset firms be subject to this Guidance, as with all traditional financial services firms. This will allow qualifying crypto firms to adequately assess whether individuals under consideration to hold SMF or Certified functions possess honesty, integrity, competence and financial soundness. This can provide both firms and the FCA with confidence that individuals are suited to hold their positions.

Question 5: **Do you agree with our proposal to apply the existing SM&CR regime to cryptoasset firms, taking into account various parallel consultations on the broader SM&CR regime to ensure consistency? If not, please explain why.**

Question 6: **Do you agree with the proposed categorisation for enhanced cryptoasset firms, such as the threshold for allowing cryptoasset custodian firms to qualify as enhanced? Should we consider other ways to categorise cryptoassets firms as enhanced?**

Operational Resilience

Overview of the current framework

3.57 Operational resilience refers to the ability to prevent, adapt, respond to, recover and learn from operational incidents and disruptions. Operational disruptions can have many causes including system failures, changes to systems, people or processes, and matters outside a firm's control.

3.58 Our existing framework for operational resilience, and our other operational resilience standards, is captured within the following Handbook areas:

Handbook reference	Title
SYSC 4	General risk management requirements
SYSC 7	Risk Control
SYSC 8	Outsourcing requirements
SYSC 15A	Operational Resilience framework

3.59 SYSC 15A is our operational resilience framework and currently applies to in-scope firms carrying out financial services activities, outlined within SYSC 15A.1.1.

3.60 SYSC 15A is technology agnostic, aims to strengthen financial stability and reduce harm to consumers from operational or technological disruptions. This includes having a clear understanding and mapping of the people, processes, technology, facilities and information needed to deliver each important business service. We expect firms to assess the risks and controls in place to support their operational resilience. We have also provided a high-level table below which outlines the key requirements firms must follow when complying with SYSC 15A for operational resilience.

3.61 Firms unfamiliar with our operational resilience framework may want to read PS21/3 (operational resilience).

3.62 SYSC 4 and SYSC 7 complement our operational resilience framework, setting out risk management and control requirements for firms to consider in maintaining robust business operations and incident management.

3.63 Additionally, SYSC 8 establishes the adequacy of a firm's arrangements against the requirements for outsourced functions. Successful operation, management and governance of outsourcing functionality is fundamental to maintaining the integrity and stability of financial firms' services.

3.64 Noting the risks and vulnerabilities outlined below, such as cyber-attacks, system outages and third-party supplier failure, it is important that firms remain operationally resilient. They should have robust processes, procedures, and systems and controls in place to react quickly if something goes wrong. Particularly given the 24/7 nature of cryptoasset markets and the potential for consumer harm or market disruption, these risks can have particularly acute impacts.

3.65 Where firms use services provided by third parties, they should seek to have arrangements in place (eg contractual agreements and continuity plans) to ensure the third party appropriately manages operational and technological vulnerabilities and that firms are able to oversee these arrangements.

Overview of the SYSC 15A Operational Resilience Framework

Requirement	Definition
Important Business Services	<p>A firm must identify its important business services which, if disrupted, could:</p> <ul style="list-style-type: none"> cause intolerable levels of harm to any one or more of the firm's clients; or pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets.
Impact Tolerances	<p>A firm must, for each of its important business services, set an impact tolerance.</p> <p>Impact tolerance means the maximum tolerable level of disruption to an important business service, as measured by a length of time in addition to any other relevant metrics, reflecting the point at which any further disruption to the important business service could cause intolerable harm to any one or more of the firm's <u>clients</u> or pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets.</p>
Strategies, processes and systems	<p>A firm must have in place sound, effective and comprehensive strategies, processes and systems to enable it to comply with its obligations.</p>
Mapping	<p>A firm must identify and document the people, processes, technology, facilities and information necessary to deliver each of its important business services.</p>
Scenario testing plan	<p>A firm must develop and keep up to date a testing plan that appropriately details how it will gain assurance that it can remain within the impact tolerances for each of its important business services.</p>
Scenario testing execution	<p>A firm must carry out scenario testing, to assess its ability to remain within its impact tolerance for each of its important business services in the event of a severe but plausible disruption of its operations.</p>
Lessons learned	<p>A firm must, following scenario testing or, in the event of an operational disruption, after such event, conduct a lessons learned exercise.</p>
Self-assessment	<p>A firm must make, and keep up to date, a written record of its assessment of its compliance with the requirements in this chapter.</p>
Governance	<p>A firm must ensure that its governing body approves and regularly reviews the Self-assessment and lessons learned exercise documentation.</p>
Communications	<p>A firm must maintain an internal and external communication strategy to act quickly and effectively to reduce the anticipated harm caused by operational disruptions.</p>

Stakeholder feedback

3.66 In developing our proposals, we have also considered feedback provided to our various published discussion/consultation papers. The majority of industry responses (87%) we received as part of DP23/4 (stablecoins) were in favour of applying SYSC 15A requirements. Additionally, they specifically highlighted the following themes:

- The need for practical guidance on their application in the context of cryptoasset firms.
- Existing regulated businesses already incorporate similar practices as those proposed by the operational resilience framework, indicating a foundational alignment.
- Emphasising the importance of comprehensive risk management frameworks, regular assessments, and staff education on cybersecurity risks.

3.67 DP25/1 (cryptoasset activities) included a question on whether we should apply our existing operational resilience framework to staking firms. Most respondents (90%) were in favour of this proposal.

Vulnerabilities and risks in the sector

3.68 The cryptoasset sector's reliance on systems and technology means that poor operational resilience can amplify the impact of operational and technological risks, leading to significant disruptions that can ultimately cause serious consumer harm if managed poorly. According to industry on-chain analysis (eg '2025 Chainalysis Crypto Crime Report', 'TRM Labs 2025 Crypto Crime Report'), about USD 2.2bn worth of cryptoassets were compromised through hacks in 2024, a 17% increase from 2023. We note, for example, the February 2025 Bybit hack, where over USD 1.5bn worth of cryptoassets were stolen after attackers exploited vulnerabilities in the firm's wallet infrastructure – underlining the importance for strong operational resilience controls across all crypto firms.

3.69 These incidents highlight the need for consistent operational resilience standards for cryptoasset firms, comparable to those applied in traditional financial services.

Summary of proposals

3.70 We propose extending our operational resilience framework to cover all cryptoasset firms, including those that would not traditionally fall within its scope under existing requirements for FSMA-authorised firms. This extends the scope of SYSC 15A beyond its current application to FSMA-authorised firms, where its scope is more limited as outlined in SYSC 15A.1.1. We note that, because of extending our framework this way, FSMA-authorised firms conducting cryptoasset activities will also be brought within the scope of this framework.

3.71 We believe this approach is proportionate given the specific risks in the cryptoasset sector as noted earlier, ensuring all cryptoasset firms meet consistent operational resilience standards and are prepared to manage disruptions effectively.

3.72 We know certain business models may be more exposed to operational disruptions or present different risk profiles. To help firms understand and apply our operational resilience framework, we are also consulting on accompanying non-Handbook guidance (within Chapter 4). The non-Handbook guidance aims to give greater clarity on how the proposed requirements will apply in a cryptoasset context, with examples that reflect the nuances of different business models.

Applying our operational resilience framework to cryptoasset firms

3.73 Cryptoasset firms face many of the same operational risks as those in the traditional financial services sector, such as system outages, cyber threats and third-party dependencies. However, there are specific technological considerations unique to cryptoassets. These include integrating distributed ledger technologies (DLT) into core systems and processes and how scenario tests are performed to ensure the underlying DLT remains resilient. We want to ensure future operational resilience requirements for these firms are balanced. We also want to minimise operational and technological risk, to protect consumers and safeguard market integrity, without undermining the underlying technology and hindering innovation.

3.74 Under the proposed framework, we would expect these firms to be operationally resilient by having a comprehensive understanding and mapping of the people, processes, technology, facilities and information necessary to deliver each important business service, including testing within set impact tolerances.

3.75 It is also essential that cryptoasset firms have strong cyber resilience measures in place to ensure they are operationally resilient, and to give consumers the highest levels of protection against potential cyber attacks. When conducting a risk management exercise against their important business services, firms should consider internationally recognised risk management frameworks for cyber resilience and understand how these may apply to their business.

3.76 To support effective cyber resilience, we encourage cryptoasset firms to consider the following best practices, among others:

- Conducting regular security assessments to identify potential security vulnerabilities in their IT infrastructure, and to remediate appropriately where they find them.
- Using strong encryption and security protocols to protect data and code.
- Implementing detection capabilities such as firewalls and intrusion detection systems.
- Patching and updating software, including smart contracts, in a timely way.
- Ensuring information is regularly backed up, and disaster recovery and business continuity plans are in place and embedded.
- Creating effective incident management plans to minimise the impact of an incident and openly share information with authorities on request.
- Having employee training programmes on cyber security to educate staff on security risks.

3.77 We want to be clear that a UK branch of an overseas firm is not in scope of SYSC 15A, as outlined in SYSC 15A.1.4[R]. In-scope UK firms that operate overseas branches may want to voluntarily apply some or all the requirements to those branches to support a consistent approach across their operations. Our other operational standards (eg outsourcing rules in SYSC 8) do apply to overseas branches.

3.78 Under our proposed rules, when a firm uses outsourced and other third-party service providers, it retains responsibility for managing risks from these arrangements. When a firm increases its dependence on these providers, it needs to increase its levels of risk management, as outlined in SYSC 8. However, we recognise that cryptoasset firms may face challenges applying SYSC 8 provisions to permissionless DLTs, due to the lack of direct contractual relationships with DLT providers. To avoid restricting the use of permissionless DLTs, we propose that such use should not be treated as an outsourcing arrangement under SYSC 8.1.1[R].

Explanatory Box:

Permissionless DLTs are ledger systems where anyone can participate in validating transactions and access the network without prior approval or permission from a central authority, which can result in less control over the underlying technology.

3.79 Additionally, where a firm relies on a third party for the delivery of an important business service, we would expect the firm to have sufficient understanding of the people, processes, technology, facilities and information that support the provision by the third party of its services to or on behalf of the firm, to allow the firm to comply with its obligations under SYSC 15A.

3.80 Our accompanying non-Handbook Guidance (within Chapter 4) outlines how we expect cryptoasset firms to apply and implement our existing operational resilience framework. It includes potential areas for consideration and gives examples for relevant cryptoasset business models.

3.81 We also plan to consult in Q1/Q2 of 2026 on non-Handbook guidance on the use of DLTs, to provide greater clarity on their implications for operational resilience.

Other operational resilience standards

3.82 Further to our operational resilience framework and outsourcing requirements, we expect firms to consider our Principles for Business (PRIN) and all other operational resilience standards (eg SYSC 4 and 7) in our Handbook to ensure they are operationally resilient.

3.83 PRIN sets out high-level general statements of the fundamental obligations for firms. They include: 'A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems' (Principle 3, PRIN 2.1).

3.84 As noted in the previous chapter, we propose that SYSC 4 and SYSC 7 be applied to cryptoasset firms as guidance, following the approach used for FSMA-authorised firms.

These provisions set out expectations for firms to manage risks and maintain strong operational controls, helping ensure business continuity and effective incident response.

3.85 Currently, FSMA-authorised trading venues must meet tailored obligations under MAR 5 and MiFID RTS 7. To ensure we retain flexibility to introduce comparable requirements for cryptoasset trading platforms, we may, where appropriate, set out our expectations in our future CP. These more specific obligations would complement, rather than replace, the above operational resilience requirements in SYSC.

3.86 We expect this approach to operational resilience will reduce consumer harm and increase market integrity. By considering impact tolerances and assessing their systems and processes, cryptoasset firms are also likely to be able to provide better customer service by identifying and responding to risks and being able to react in the event of operational disruption.

Reporting requirements

3.87 Currently, when firms experience incidents, they need to fulfil their obligations to us under Principle 11 and the SUP 15.3 General Notification Requirements by reporting these incidents.

3.88 Our CP24/28 (incident reporting) sets out proposed reporting rules that clarify the types of operational incidents all firms should report. The new third party reporting requirements apply only to in-scope firms carrying out financial services activities (like SYSC 15A).

3.89 The proposed improvements to operational incident reporting will apply to all firms. However, we also want to propose the extension of third-party reporting requirements to all cryptoasset firms. This would ensure that both FSMA-authorised firms and cryptoasset firms follow a consistent approach, in line with our principle of 'same risk, same regulatory outcome'.

3.90 We recognise that this proposal may prompt questions or require further clarification. We intend to consult on these reporting requirements in a future CP. We also note the collective work on operational incident and outsourcing and third-party reporting being undertaken by the FCA, Bank of England and Prudential Regulation Authority.

Question 7: **Do you agree with our proposal to extend the application of SYSC 15A to cover all cryptoasset firms, including FSMA-authorised firms carrying out qualifying cryptoasset activities? If not, please explain why.**

Question 8: **Do you agree with our proposal that the use of permissionless DLTs by cryptoasset firms should not be treated as an outsourcing arrangement? If not, please explain why.**

Financial Crime

Overview of the current framework

3.91 Since January 2020, cryptoasset businesses operating in the UK (defined in the Money Laundering Regulations (MLRs) as cryptoasset exchange providers or custodians (wallet providers) have been required to register with us. As well as complying with the anti-money laundering (AML), counter terrorist financing (CTF) and counter proliferation financing (CPF) obligations in the MLRs, they also need to comply with other relevant legal requirements under financial crime legislation. These include the requirements under the Terrorism Act 2000, and the Proceeds of Crime Act 2002.

3.92 As part of their obligations under the MLRs, registered firms must demonstrate that they have adequate systems, controls, policies, and procedures in place to effectively manage the risks of money laundering, terrorist financing and proliferation financing in the cryptoasset market. They must also comply with the Travel Rule following its introduction in September 2023.

3.93 Cryptoasset firms will still be subject to the MLRs, as well as the other financial crime-related legal requirements above. As outlined in Treasury's policy note accompanying the draft SI and MLR consultation responses, they will no longer be required to register separately with the FCA as cryptoasset businesses under the MLRs. Rather, they will need to be authorised by us under FSMA.

3.94 As in previous SYSC proposals outlined in this chapter, we propose that cryptoasset firms, similar to FSMA-authorised firms, should be subject to FCA Handbook Rules and Guidance including those on Financial Crime. This means that cryptoasset firms will have to follow both statutory obligations and our Handbook requirements outlined in SYSC 6, FCG and FCTR.

Stakeholder feedback

3.95 In DP23/4 (stablecoins) we discussed applying the existing financial crime framework to stablecoin issuers and cryptoasset custodians. In CP25/14 (stablecoin issuance and crypto custody), we discussed how our proposed redemption requirements for qualifying stablecoin issuers would interact with AML, CTF, and CPF obligations.

Vulnerabilities and risks in the sector

3.96 Since 2020, the National Crime Agency (NCA) has seen a significant increase in money laundering through cryptoassets. The cross-border and fast-moving nature of the blockchains and cryptoasset transactions present unique difficulties for effective detection and enforcement against criminal actors and sanctioned entities. This can make cryptoassets more appealing to criminals and sanctioned entities as they perceive a lower likelihood of detection.

3.97 The NCA also acknowledged in their 2025 National Strategic Assessment of Serious and Organised Crime that cryptoassets are increasingly used to launder non-digital

proceeds of crime, such as cash, and are acquired via increasing levels of cybercrime – such as theft, malware, and ransomware. The NCA also reported that between USD 1.7bn – USD 5.1bn a year in illicit cryptoasset transactions are estimated to be linked to the UK.

3.98 As outlined in Chapter 1, the [2025 National Risk Assessment \(NRA\) for Money Laundering and Terrorist Financing](#) has also ranked the risk for cryptoassets as 'high' and 'medium' respectively.

3.99 According to industry on-chain analysis ([2025 Chainalysis Crypto Crime Report](#)), 2024 saw a total of USD 40.9bn in value received by illicit cryptoasset addresses. Since 2020, annual estimates of illicit activity have grown by an average of 25% between each annual reporting periods.

3.100 This underscores the need for cryptoasset firms to implement strong financial crime controls that match the standards applied to traditional financial services.

Summary of proposals

3.101 We consider it proportionate for cryptoasset firms to be subject to the same financial crime rules in place for other FSMA authorised firms. We believe the financial crime framework that applies to traditional finance firms adequately addresses the risks we have seen in the cryptoasset market, such as crimes including fraud and scams, money laundering, terrorist financing, proliferation financing, and sanctions evasion.

3.102 We propose applying the rules and guidance in SYSC 6 to ensure that cryptoasset firms have adequate policies and procedures, including systems and controls to identify, assess, monitor and manage money laundering risks. We expect policies and procedures to be comprehensive and proportionate to the nature, scale and complexity of firms' activities.

3.103 Requiring firms to implement robust policies to manage money laundering, terrorist and proliferation financing risks, as well as regularly reviewing these policies' effectiveness, will help cryptoasset firms to reduce the level of illicit activities more widely in this sector.

3.104 We also propose applying the guidance contained in the Financial Crime Guide (FCG) and the Financial Crime Thematic Reviews (FCTR) to cryptoasset firms, so they have practical help and information on actions they can take to counter financial crime risks.

Applying our financial crime framework to cryptoasset firms

Handbook reference	Title
SYSC 6.1.1 R	Adequate policy and procedures
SYSC 6.3.1 R	Financial Crime – systems and controls
SYSC 6.3.3 R	Financial Crime – systems and controls assessments
SYSC 6.3.8 R	Financial Crime – senior manager responsibility
SYSC 6.3.9 R	Financial Crime – Money Laundering Reporting Officer

Question 9: Do you agree with our proposal to require cryptoasset firms to follow the same financial crime framework as FSMA-authorised firms? If not, please explain why.

3.105 The proposals in this chapter for implementing robust governance requirements, a personal accountability framework, operational resilience standards, and Financial Crime requirements that go beyond those already entailed within the MLRs, aim to improve and promote compliance culture in this sector. Our proposals will allow cryptoasset firms to build stronger systems and controls, giving them opportunities to detect incidents early and better respond to disruption or failures. Overall, our proposals will help firms to manage the particular vulnerabilities and risks in this market.

Chapter 4

Guidance on cryptoasset operational resilience

Introduction

4.1 Operational resilience is fundamental to the integrity and stability of financial services. The cryptoasset sector relies heavily on digital technology to deliver services, and support system and infrastructure to conduct their activities.

4.2 In Chapter 3, we proposed applying our existing operational resilience framework to cryptoasset firms. This includes the following requirements and standards:

1. SYSC 4 (General Risk Management Requirements)
2. SYSC 7 (Risk Control)
3. SYSC 8 (Outsourcing)
4. SYSC 15A (Operational Resilience Requirements)

4.3 This chapter provides guidance to firms to help them implement our operational resilience requirements (SYSC 15A), with reference to our outsourcing provisions under SYSC 8, under the cryptoasset regime. To ensure this guidance is relevant for cryptoasset firms, we will focus on:

- a. Cryptoasset-specific operational and technological risks that, due to the unique characteristics of cryptoassets, may happen more often in the cryptoasset sector than in traditional financial services, presenting distinct challenges for firms.
- b. Using example cryptoasset business models to demonstrate how operational resilience requirements can apply in practice within regulated cryptoasset activities, giving firms examples of how they can build resilience.

Cryptoasset-specific operational & technological risks

4.4 While many operational and technological risks are common in both traditional financial firms and cryptoasset firms, the unique characteristics of cryptoassets introduce specific challenges. The table below highlights some of these. This is not a complete list and is intended to provide an initial overview; we will explore each risk further throughout the guidance to help firms in building operational resilience.

Private key security risks	Private key security risk refers to the risk of unauthorised access to private keys, which may result in the loss or theft of cryptoassets. For example, cyber attacks may expose private keys, enabling the attacker to steal consumers' cryptoassets. These attacks can occur if virtual wallets storing private keys are not adequately protected, for example, due to weak access controls.
Validator risks	Validator risk arises when cryptoasset firms rely on validators (eg for staking) without conducting appropriate due diligence or ensuring adequate controls. Misconduct or operational failures by validators, such as double signing, can lead to slashing penalties (having a portion of staked assets forfeited) and loss of staked assets for the firm and its clients.
Code vulnerabilities	Use of code (eg smart contracts) can potentially make cryptoasset firms vulnerable to hacks if they do not adequately test, review and update the underlying code on an ongoing basis.
Service disruptions	Service disruption risks involve disruptions to services or underlying technologies (such as distributed ledger technology) which prevent consumers from accessing or transacting with their cryptoassets when needed. This can leave consumers unable to sell during price volatility or make time-sensitive payments, leading to financial loss.

Example firms

4.5 We use 4 fictional example firms in this document to illustrate how our requirements might apply to different types of firms conducting or supporting regulated cryptoasset activities. While these examples are illustrative, the risks and scenarios described may be applicable across all example firms.

Firm A: Qualifying Stablecoin Issuer

Firm A is a qualifying stablecoin issuer that issues a stablecoin referenced to a fiat currency. The firm's business model involves offering the stablecoin to the public, undertaking the redemption and maintaining the value of the stablecoin (eg managing the backing assets). The issuer has created their stablecoin on multiple permissionless DLTs.

The firm has used inbuilt smart contracts within the stablecoin's token structure, enabling them to freeze stablecoins if stolen or linked to illicit activity, helping to improve security and general compliance against their regulatory requirements.

Firm B: Qualifying Cryptoasset Trading Platform

Firm B operates a cryptoasset trading platform providing services to retail and institutional clients. Retail clients can make simple buy-and-sell transactions through an intuitive online interface. Institutional clients receive direct access to advanced trading services via dedicated interfaces and APIs, enabling automated and algorithmic trading. Firm B maintains robust order-matching systems, liquidity pools and secure omnibus cryptoasset wallets.

As part of their Know Your Customer (KYC) processes, Firm B outsources client identity verification to a specialised third-party provider, maintaining clear service-level agreements. Firm B retains internal oversight of outsourced services, regularly evaluates provider performance and ensures the arrangement supports operational continuity and regulatory compliance.

Firm C: Qualifying Cryptoasset Staking

Firm C offers custodial staking services to retail and institutional clients across multiple proof-of-stake (PoS) blockchain networks. Clients place their cryptoassets into Firm C's platform, where the firm handles all aspects of the staking process on their behalf.

Rather than running its own validator nodes (systems that validate transactions and secure the blockchain in return for rewards), Firm C outsources the operation of validator nodes, delegating clients' cryptoassets to a network of third-party validator operators under formal outsourcing arrangements. These third parties manage the infrastructure and participate in network consensus on Firm C's behalf.

As a custodial service, Firm C also stores private keys associated with the staked cryptoassets, implementing controls to maintain secure storage and controlled access for clients.

Firm D: Cryptoasset Custody

Firm D provides cryptoasset custody services to retail and institutional clients, safeguarding a broad range of cryptoassets across multiple blockchain networks. Clients deposit cryptoassets with Firm D to hold or store the means of access to the cryptoasset, ie to protect the private key used to access the cryptoasset. It operates a hybrid storage architecture that combines cold and hot wallet infrastructure.

Cold wallets are used for long-term storage. Hot wallets are used to support real-time transactional activity. Firm D uses multi-party computation (MPC) to split and secure cryptographic keys across multiple systems, reducing the risk of compromise.

In addition to custody, Firm D offers clients real-time reporting tools and maintains recovery plans for loss of access or security breaches. Clients engage solely through Firm D's platform, which acts as their single point of access, while the firm manages all interactions with underlying blockchain networks on their behalf.

Operational resilience framework Guidance

4.6

Firms engaged in cryptoasset activities should apply the principles in SYSC 15A, such as when identifying Important Business Services, setting impact tolerances, mapping dependencies and conducting scenario testing. The table below illustrates sound operational risk management practices and should inform each stage of our operational resilience framework:

Key Focus Area	Expectations for Cryptoasset Firms
Cyber and Technology Resilience	Firms should maintain robust and proportionate cyber and IT controls to ensure their systems which support cryptoasset related services are resilient. This includes managing risks to system availability, data integrity, third-party dependencies and using recognised international cyber security standards and relevant best practices.
Safeguarding Cryptographic Keys and Infrastructure	Where firms hold or store the means of access to the cryptoasset (eg private keys), including any supporting infrastructure to provide this service (eg smart contracts or validator nodes), they should establish secure and well-defined processes. These processes should address the management of private key loss, unauthorised system access, and general service disruptions. We expect firms to adopt and maintain high technical standards to safeguard both private keys and the resilience of the underlying infrastructure as outlined above.
Continuity and Disruption Planning	Firms should create, test, and regularly update plans to maintain or restore critical services during disruptions. Scenarios should reflect cryptoasset activities that a firm carries out and the underlying infrastructure to support the service (eg smart contract failure, failure in the technology to support stablecoin reconciliation processes and validator outages). Targeted vulnerability scans and penetration tests should be carried out to identify and address risks.

4.7 This guidance should be read alongside our final Policy Statement(s) on our cryptoasset regime, and PS21/3 (operational resilience), which complements this guidance by covering broader, non-crypto considerations.

Outsourcing expectations for Cryptoasset Firms

4.8 When reading the guidance below, cryptoasset firms should also consider our outsourcing requirements under SYSC 8. SYSC 8 defines outsourcing as 'an arrangement of any form between a firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the firm itself.'

4.9 As such, firms should read each section of this guidance with SYSC 8 in mind and, as per SYSC 8.1.11A[G] apply appropriate skill, care, and diligence to outsourced arrangements. They should consider the nature, scale and complexity of those arrangements in the context of their operational resilience planning. This includes arrangements with both traditional service providers and other technology providers where relevant.

4.10 However, recognising the challenges of applying the above definition to permissionless DLTs, and as proposed in chapter 3 of this consultation paper, the use of permissionless DLTs should not be treated as an outsourcing arrangement under SYSC 8.1.1[R].

4.11 Nevertheless, we expect cryptoasset firms to evaluate their internal operational controls for permissionless DLTs, following the operational resilience framework in SYSC 15A and the guidance below. Ultimately, firms remain responsible for maintaining their own operational resilience.

Identifying important business services

4.12 SYSC 15A.2.1[R] states that all firms within scope of SYSC 15A must clearly identify their important business service to ensure they can remain operationally resilient. As outlined in the previous chapter, this requirement also applies to cryptoasset firms, along with all subsequent requirements set out below.

4.13 As defined in SYSC 15A, an Important Business Service means a service provided by a firm, or by another person on behalf of the firm, to one or more clients of the firm which, if disrupted, could:

1. Cause intolerable levels of harm to any one or more of the firm's clients, or
2. Pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets.

Factors to consider when identifying important business services

4.14 Cryptoasset firms may rely on third parties to deliver their important business service. Firms must ensure these services are appropriately identified, mapped and tested in line with our operational resilience requirements. Additionally, firms still remain fully responsible for following our requirements in cases where the third party may be decentralised (eg permissionless DLTs) and firms have limited control over the third party.

4.15 Where a cryptoasset firm performs multiple activities (eg a cryptoasset trading platform that also offers custody and staking services), the delivery of these activities is likely to be underpinned by multiple important business service. Firms should clearly identify each of these separate important business service.

4.16 Cryptoasset firms often primarily serve retail customers, some of whom may be particularly vulnerable to service disruptions, especially where outages prevent transactions from completing or disrupt essential services (eg where stablecoins are used for payments).

4.17 We are also seeing cryptoasset services becoming more closely interconnected with traditional financial markets (eg traditional custodians safeguarding stablecoin backing assets), increasing the potential for wider market contagion if disruptions occur. Given these specific considerations, firms should adopt a holistic approach when identifying their important business service, taking into account the full, non-exhaustive list of relevant factors set out in SYSC 15A.2.4[G].

4.18 Correctly identifying these important business service is the foundation for complying with our operational resilience framework and ensuring operational risks are appropriately accounted for and managed.

How our example firms might identify important business services

Firm A

Firm A, the stablecoin issuer, identifies the redemption of its fiat-referenced stablecoin as one of its important business services. Holders rely on Firm A to convert stablecoins back into money and for the firm to place a payment order to return the money to the client.

A disruption to this service could prevent a holder from accessing the redemption amount. Additionally, given the role of stablecoins in potentially enabling payments and trading activity across cryptoasset markets, a public disruption could also undermine confidence in the stablecoin and contribute to broader market instability.

Firm B

Firm B, the cryptoasset trading platform, identifies the execution of orders as one of its important business services. Market participants rely on the platform to execute trades efficiently and at expected prices.

A failure in this service could disrupt market liquidity, impair price formation and cause financial losses for clients. Prolonged disruption may also undermine confidence in the platform and contribute to instability across other firms connected to the platform.

Firm C

Firm C identifies the operation of validator nodes, managed by third-party technology providers, as one of its important business services. Clients rely on Firm C to stake their cryptoassets and earn rewards through these validator nodes.

If the third-party providers fail to run the nodes properly, Firm C may be unable to perform key functions such as distributing rewards and could face slashing penalties. This could cause financial loss to consumers and affect Firm C's ability to operate its business.

Firm D

Firm D, the cryptoasset custody provider, identifies providing and managing secure custody solutions as one of its important business services. Clients depend on Firm D to safeguard their cryptoassets and for continued access to them.

A disruption could prevent clients from accessing their assets when needed, leading to financial loss, reduced liquidity and greater exposure to market volatility. This may also affect other firms that rely on timely asset transfers or settlement, increasing the risk of wider disruption.

Setting impact tolerances

4.19 Once a firm has identified their important business service, SYSC 15A.2.5[R] requires them to clearly define impact tolerances for each of its important business service. Impact tolerances represent the maximum level of disruption a firm judges acceptable before harm occurs to consumers, market integrity or financial stability that exceeds what the firm considers tolerable.

4.20 Cryptoasset firms must also ensure they can maintain their impact tolerance for each of their important business service if there is a severe but plausible operational disruption, in accordance with SYSC 15A.2.9[R].

Factors to consider when setting impact tolerances

4.21 Cryptoasset firms should establish a clear scale, measured by a length of time and any other relevant metrics, that determines how long an important business service can be disrupted before the firm exceeds its impact tolerance. Firms should calibrate these tolerances to reflect the nature of their services and associated risks.

4.22 As set out in SYSC 15A.2.8[G], when setting impact tolerances, cryptoasset firms should consider how demand for each of their important business service may fluctuate, particularly during periods of heightened market activity. For example, cryptoasset markets operate 24/7 and can experience sudden spikes in trading volumes. Firms should ensure their impact tolerances are appropriately calibrated to reflect these fluctuations, including periods of peak demand, to maintain operational resilience under the most severe but plausible conditions.

4.23 As cryptoasset firms often operate multiple services, there may be instances where the service suffers multiple disruptions within a short timeframe. Nevertheless, firms are expected to set their impact tolerances with reference to a single disruption event, rather than an aggregate of multiple disruptions. This approach is essential to ensure impact tolerances remain a precise and reliable metric for the maximum level of disruption that can be tolerated.

4.24 Firms must monitor their impact tolerances on an ongoing basis and, where these are breached, ensure that appropriate business continuity and contingency plans are in place to manage and mitigate harm.

4.25 Firms should also note SYSC 15A.2.7[G], which outlines a sample list of factors to consider when setting their impact tolerances.

Use of third parties and multiple disruptions when setting impact tolerances

4.26 As noted in the previous section, when a firm uses a third-party provider in the delivery of an important business service, they should work effectively with the third-party to agree set impact tolerances. A firm should ensure the provider remains within those tolerances and monitors its performance against those tolerances on an ongoing basis. Where that is not possible (for example, when using a decentralised service), the responsibility for setting and remaining within impact tolerances remains with the firm.

4.27 Setting accurate impact tolerances ensures firms can effectively prevent, adapt, respond to and recover from operational disruptions.

Resuming a degraded service

4.28 A degraded service means a partially functioning service operating below full capacity. SYSC 15A.2.10[G] advises that cryptoasset firms should have clear plans and criteria for resuming a degraded service during disruptions. Firms should consider running a degraded service when the risks of not doing so are greater.

4.29 Given the complexities of cryptoasset business models, firms are encouraged to carefully assess and test when, and how, resuming a degraded service may reduce intolerable harm while balancing broader operational and security considerations. We provide examples below:

- **A cryptoasset trading platform suffers a disruption following a cyber attack.**

To minimise harm to clients and maintain market confidence, it makes a strategic decision to partially restore trading functionality in a degraded mode. While full trading is not available, users can still access account balances and make limited withdrawals.

The firm determines that this limited functionality reduces the risk of consumer harm without compromising the platform's security. Throughout the incident, the firm communicates transparently with clients, clearly setting expectations about service limitations while it works to safely restore full operations.

- **Following a critical incident affecting its infrastructure provider, a cryptoasset custody firm loses access to part of its key management system,** temporarily halting withdrawal processing. Rather than rushing to resume full service, the firm conducts an impact assessment and determines that partial restoration can support clients without compromising asset security.

The firm enables read-only access to customer wallets and transaction histories, helping users verify asset holdings and account activity. Withdrawals remain paused to avoid introducing further risk while forensic checks are completed. By restoring this limited functionality, the firm reduces uncertainty and supports customer confidence during the disruption.

How our example firms might set impact tolerances

Firm A

To set an impact tolerance, **Firm A** considers the potential harm if there is a failure in the underlying DLT. It identifies that consumer harm is the most relevant, given the number of consumers affected and their reliance on the service to redeem their stablecoins to money. Using redemption rate forecasts, Firm A concludes that being unable to process redemptions over an 8-hour period, due to system outage, would be outside the firm's impact tolerance. A delay to processing redemption requests within this period would lead to significant disruption and therefore an intolerable risk of consumer harm.

Firm B

Firm B has identified that disruption to its cryptoasset trading platform could lead to considerable consumer harm. Clients rely heavily on uninterrupted access to simple buy-and-sell transactions to manage their cryptoasset holdings effectively. Recognising the critical need for ongoing service availability, Firm B considers the maximum tolerable period for disruption to its trading platform, including the order-matching systems and access to hot wallet storage, should be set somewhere between 1-24 hours (depending on the scale of the disruption). This timeframe reflects the rapid nature of cryptoasset market transactions, reducing the risk of financial losses and disruption of liquidity.

Firm C

To set an impact tolerance, **Firm C** works closely with its third-party providers to understand potential harm. Firm C identifies consumer harm as the main risk, given clients' reliance on staking rewards and the possibility of financial loss if rewards are missed or penalties occur. If a validator goes offline, rewards stop and do not accrue until service resumes. Prolonged downtime can also lead to penalties such as slashing. Firm C reviews validator performance, reward timing and disruption durations that could cause these outcomes.

Based on this, Firm C sets a time-based impact tolerance, such as a maximum disruption of 24–48 hours, after which consumer harm would be intolerable. Firm C maintains regular communication with its providers to ensure the impact tolerance can be met during disruptions.

Firm D

To set an impact tolerance, **Firm D** considers the potential harm to clients if they cannot access their wallets. Clients depend on continuous access to both hot wallets, for transactional activity, and cold wallets, for secure long-term storage. A disruption could result in missed trading opportunities, liquidity constraints or financial loss during periods of market volatility.

Firm D analyses typical wallet usage patterns, including transaction volumes and withdrawal frequencies. It also considers the potential for disruptions to affect multiple services that depend on custody, amplifying the overall impact. Using a time-based metric, Firm D sets its impact tolerance at 4 hours, subject to firm-specific factors such as systems and technologies used.

Mapping exercises

4.30 Under SYSC 15A.4.1[R], cryptoasset firms must identify and document the people, processes, technology, facilities and information necessary to deliver each of their important business service. This mapping must be sufficiently detailed to support effective impact tolerance testing and help firms understand their vulnerabilities.

4.31 For further information on the definitions of people, processes, technology, facilities and information, please refer to PS21/3.

Examples of cryptoasset-specific vulnerabilities identified via mapping

4.32 Given the nature of cryptoasset business models – including features such as decentralisation, third-party reliance and evolving technologies – firms should pay particular attention to the unique risks and vulnerabilities involved when mapping their technologies:

- Unavailability of critical third-party services like DLT providers (especially in the case of permissionless DLTs), including business-continuity plans and off-chain controls.
- Significant technology disruptions affecting cryptoasset transaction processing (eg smart contract failures or blockchain outages).
- Loss or reduced provision of critical infrastructure supporting cryptoasset services (eg failure of primary trading platform infrastructure).

4.33 Cryptoasset firms remain fully responsible for accurately mapping any relationships with third parties. Where a firm relies on external providers – such as custodians, validators, off-chain oracle services, or fiat on/off-ramp partners – it must be able to identify and understand any vulnerabilities in those arrangements, whether they lie directly with the third party or further along the service chain.

4.34 However, third parties may be decentralised and lack direct contractual agreements, such as some permissionless DLTs or decentralised protocol developers. In these cases, firms must strengthen internal controls and monitoring to identify and address vulnerabilities beyond traditional oversight. This may involve enhanced transaction monitoring across on-chain and off-chain activities, stress-testing node connectivity, and performing regular independent audits of smart contracts.

4.35 As the cryptoasset sector expands and novel technologies are introduced, and as also outlined in SYSC 15A.4.3[R], we expect firms' mapping exercises to develop and evolve over time.

How our example firms may approach the mapping exercise

Firm A

Firm A maps the key components that support its important business service of stablecoin redemption. This includes on-chain smart contracts governing redemption mechanics, custodians holding reserve assets (an independent custodian to ensure the stablecoin is always fully backed and can be redeemed in a timely manner), external banking partners managing fund flows and off-chain monitoring systems ensuring compliance and liquidity.

The firm identifies critical third-party dependencies such as custodians holding backing assets, noting that any disruption in these areas could affect its redemptions. Firm A also maps relevant people and processes responsible for KYC checks, transaction validation and customer support.

Firm B

Firm B maps the critical components supporting its important business service of order execution and settlement. This includes trading engine infrastructure, market data feeds, order management systems and blockchain networks used for settlement.

The firm identifies key third-party dependencies such as liquidity providers, external price oracles and custodial wallets enabling asset transfers. The firm gives particular attention to vulnerabilities like technology outages, smart contract failures or latency in settlement confirmations that could disrupt order flow or settlement finality.

Firm C

Firm C maps the key components that support its important business service of validator node operation. This includes internal systems for staking management, custody of clients' cryptoassets and private keys, and interfaces with third-party validator infrastructure.

Firm C identifies its reliance on third-party technology providers as a key vulnerability, particularly the risk of downtime, performance degradation or misconfiguration leading to missed rewards or slashing.

It also recognises that limited visibility into the validator's underlying infrastructure and controls can hinder timely response to incidents. This mapping supports Firm C's understanding of where operational risk lies across the service chain.

Firm D

Firm D maps the full range of components involved in its cryptoasset custody service. This includes hot wallet infrastructure supporting real-time transactional access, cold storage vaults for secure asset safeguarding, key management systems, and third-party service providers such as hardware security module (HSM) vendors.

The firm highlights vulnerabilities such as reliance on permissionless DLTs and concentration risk among its custodial partners. Firm D's mapping also covers internal teams responsible for wallet access control and incident response.

Conducting scenario planning and testing

4.36 As outlined in the previous mapping section, firms must first identify and map the resources that underpin their important business service. Building on this, SYSC 15A.5 requires firms to develop a scenario testing plan and carry out this testing to assess their ability to remain within the impact tolerances set for each important business service.

4.37 This section focuses on the requirements for both planning and executing scenario tests, incorporating considerations of the mapped resources and associated processes.

Scenario testing planning

4.38 In line with SYSC 15A.5.1[R], cryptoasset firms must develop a clear, detailed and regularly updated testing plan that sets out how they will gain assurance of their ability to remain within impact tolerances for each of their important business service. Given the rapid pace of innovation in the cryptoasset sector, regular updates to the testing plan are essential to maintaining effective operational resilience.

4.39 When developing this plan, firms should consider the partial list of considerations set out in SYSC 15A.5.2[G]. Given the nature of cryptoasset business models, firms should pay particular attention to designing testing scenarios that reflect their specific risks and operational dependencies, such as trading platform outages, stablecoin redemption delays or failures in staking service delivery.

Scenario testing execution and documenting lessons learned

4.40 Complementing the scenario testing planning, firms must also execute scenario tests – as required under SYSC 15A.5.3[R] – to assess their operational resilience under severe but plausible disruption scenarios. Testing should include a diverse range of adverse circumstances varying in nature, severity and duration, relevant to cryptoasset business models.

4.41 Additionally, in line with SYSC 15A.5.6[G], firms should, among other things, aim to cover scenarios such as:

- Data corruption or loss (eg manipulation of wallet balances or transaction records)
- Critical third-party outages (eg custodian or blockchain node service disruptions), and
- Failures in the technology (eg malicious node activity or oracle manipulation) and/or people (eg insider threats) supporting their important business services.

4.42 When conducting scenario testing involving third parties, firms must ensure third-party testing methodologies are valid, effective and aligned with the firm's operational resilience requirements. However, where testing directly with a third-party service provider (like permissionless DLTs) is not possible, firms should use best alternatives where possible as they still remain responsible for following our requirements.

4.43 Following each test, and where actual operational disruption occurs, firms must conduct a lessons learned exercise in line with SYSC 15A.5.8[R]. This should identify any weaknesses exposed during testing or disruption and inform actions to improve the firm's ability to respond to and recover from future incidents.

How our example firms might conduct scenario testing

Firm A

Firm A conducts regular reviews of resources that enable it to deliver its important business services as part of its annual business impact analysis. It designs severe but plausible scenarios, considering the potential impact of the redemption service and engages with the underlying DLT provider, including exploring ways to communicate with permissionless DLT communities where feasible.

These tests indicate some residual risks and resilience gaps when faced with a severe but plausible scenario including those from DLT facing long-term disruption. Following a review of lessons learned, Firm A notes that it could use other DLTs as an additional service delivery channel to enable on-chain redemption.

Among other actions, the firm also conducts a benchmarking exercise to identify alternate third-party firms that could enable redemption if the issuer has other technological issues.

Firm B

Firm B carries out scenario tests that simulate failures in its order-matching engine and distortions in market data feeds. These tests cover severe but plausible scenarios, including sudden surges in trading volume, latency issues and outages at key third-party data providers. The firm assesses its ability to maintain order integrity, switch to secondary trading infrastructure and preserve price accuracy for both retail and institutional clients. Post-test analysis identifies a dependency on a single market data aggregator as a resilience gap. As a result, Firm B begins onboarding an additional provider and invests in internal tools to support price validation across multiple sources.

Firm C

Firm C develops and maintains a scenario testing plan to assess its ability to remain within impact tolerance for its important business service of validator node operation. Scenarios include prolonged downtime or slashing events affecting its third-party technology providers. As Firm C does not control validator infrastructure, its testing focuses on internal communications and controls. Simulated slashing scenarios are used to assess how effectively Firm C informs clients, manages internal escalation and maintains service transparency. Lessons-learned exercises help improve client messaging, internal coordination and monitoring processes.

Firm D

Firm D conducts scenario tests simulating a range of severe but plausible scenarios affecting its custody services. These include hot wallet compromises, cold storage access failures and internal access control breaches. These exercises validate Firm D's ability to isolate affected infrastructure, initiate backup procedures and restore access using secure off-site recovery systems. The tests also assess the resilience of its MPC protocols and coordination of its incident response and compliance teams. As part of lessons learned, the firm identifies a gap in its visibility over outsourced key management hardware. In response, Firm D formalises assurance procedures with its third-party vendor and implements additional internal controls to independently verify the health and activity of its custody infrastructure.

Communications

4.44 SYSC 15A.8 outlines effective communication strategies that are critical for cryptoasset firms to manage operational disruptions successfully and minimise harm to clients and other stakeholders. While these requirements and guidance are clear as currently set out, we have outlined examples below. These illustrate key scenarios where timely, transparent and technically-informed external and internal communication is essential to maintaining trust and ensuring clients are adequately supported.

4.45 Example of disruptions requiring effective communication:

- **Disruptions outside the firm's control:** When operational disruptions arise from factors beyond the firm's direct control, such as a blockchain fork, clear and timely communication with clients is vital. Firms should promptly inform clients of the

disruption, explain potential impacts on services or cryptoasset holdings, and provide guidance on any actions clients may need to take. They should provide regular updates throughout the event to ensure transparency and maintain client confidence.

Explanatory Note – Blockchain Forks:

A fork occurs when a blockchain splits into 2 competing chains. The causes of forks can vary. In some cases, forks result unintentionally from the simultaneous creation of competing blocks, leading to a temporary divergence in the blockchain (hard forks). In other instances, forks are deliberate protocol upgrades that modify the rules governing the creation of new blocks (soft forks). For users of the blockchain, forks can lead to temporary disruptions, such as transaction delays or confusion over which chain to follow and may sometimes require them to take action to ensure their assets remain secure and accessible.

- **Cyber security breach:** If a targeted hacking attack occurs, for example, unauthorised access to wallets, firms must promptly notify affected clients and stakeholders (eg through the firm's website and email notifications). Communications should include a clear summary of the incident, including the nature and scope of the breach, immediate containment actions (eg freezing transfers, isolating affected systems), and client-specific steps (eg resetting 2 factor authentication, monitoring withdrawal history). Ongoing updates should outline the status of forensic investigations, progress on asset recovery, and improvements to security controls.

4.46 This guidance aims to help cryptoasset firms develop and implement our operational resilience framework, helping them to maintain critical services, protect consumers and contribute to the stability of financial markets, even during periods of disruption. However, this guidance is not a complete description of the steps firms should take when ensuring operational resilience. Ultimately, it is up to firms to determine the extent of the analysis or review they need to confirm they meet our operational requirements in SYSC 15A.

Question 10: **Do you agree with the guidance set out in this document, and can you outline any areas where you think our approach could be clearer or better tailored to the specific risks and business models in the cryptoasset sector?**

Question 11: **Are there any emerging digital and cyber security industry practices or measures which we should consider when supporting cryptoasset firms complying with operational resilience and related requirements? Please elaborate.**

Chapter 5

Business standards

Applying the Environmental, Social and Governance Sourcebook to cryptoasset firms

5.1 The ESG Sourcebook ensures FSMA-authorised firms provide clear, accurate, and consistent information about the sustainability characteristics of their products and services and how they manage climate and sustainability risks and opportunities.

5.2 We propose to apply the ESG Sourcebook to cryptoasset firms in the same way as it applies generally to all FSMA-authorised firms. This means that cryptoasset firms will be subject to requirements under ESG 4.1.1R and ESG 4.3.1R.

5.3 We do not propose to extend ESG provisions that only apply to specific firm types, such as asset managers, asset owners, and distributors, to cryptoasset firms. We also do not propose to introduce new cryptoasset-specific climate related or sustainability disclosure requirements for this sector at this time.

Environmental, Social and Governance (ESG)

Overview of the current framework

5.4 The ESG Sourcebook includes requirements for firms communicating or approving financial promotions in the UK. The anti-greenwashing rule (ESG 4.3.1R) applies broadly to all FSMA-authorised firms and requires that sustainability claims must be fair, clear and not misleading. ESG 4.1.1R also applies to all FSMA-authorised firms, stating that firms must not use a sustainability label unless they are asset managers that are meeting the relevant conditions.

5.5 Additionally, the ESG Sourcebook sets out rules and guidance on climate and sustainability-related disclosures, sustainability labelling, naming, and marketing. These rules apply to asset managers, asset owners and distributors.

Stakeholder feedback

5.6 In developing our proposals, we considered feedback to our previous publications, including [DP24/4](#) (A&D and MARC), which proposed requirements for firms to disclose information on the sustainability impact of cryptoassets they offer. Respondents highlighted several challenges, including difficulty getting reliable data, limited demand for this information among crypto users and the risk of placing unnecessary burdens on cryptoasset firms.

Vulnerabilities and risks in the sector

5.7 Cryptoasset activities can be environmentally intensive, especially those using Proof-of-Work (PoW) blockchains. Proof-of-Stake (PoS) is more energy-efficient but still relies on data centres that consume electricity for operation and cooling.

Summary of proposals

5.8 We propose that ESG rules applicable to all FSMA-authorised firms will also apply to cryptoasset firms. These rules apply by virtue of FSMA authorisation and are not based on environmental impact alone.

5.9 Under ESG 4.3.1R, cryptoasset firms promoting cryptoassets and associated products and services to UK customers will need to ensure any claims about sustainability characteristics of those products are fair, clear and not misleading. This aligns with our existing financial promotion rules and helps prevent greenwashing so people can trust the information they receive. Under ESG 4.1.1R, cryptoasset firms would not be able to use a sustainability label.

5.10 Where the ESG Sourcebook applies to specific types of firms such as asset managers, we do not propose to extend these provisions to cryptoasset firms. This reflects the differing nature of cryptoasset activities compared to the types of firms subject to specific requirements under the ESG Sourcebook.

5.11 We do not currently propose to introduce new climate-related or sustainability disclosures for cryptoasset firms. This approach reflects the early stage of the crypto market and stakeholder feedback suggesting it is difficult to get sustainability data and that there is no clear demand. On this basis, we do not think that mandating disclosures would lead to more informed decision making by crypto users.

Question 12: Do you agree with our proposal to apply the ESG Sourcebook to cryptoasset firms?

Chapter 6

Discussion Chapter – Applying the Consumer Duty and access to the Financial Ombudsman Service to regulated cryptoasset activities

6.1 This chapter contains a discussion on applying the Consumer Duty (the Duty) and whether customers of cryptoasset firms should be able to refer complaints to the Financial Ombudsman Service ('Financial Ombudsman'). It sets out some of the issues which may require further consideration.

The Consumer Duty

6.2 Since its introduction on 31 July 2023, the Duty has set high standards of retail consumer protection across financial services. It encourages firms to go beyond narrow rule compliance and focus on delivering good outcomes for retail consumers, setting robust expectations that apply to products and services offered to retail customers.

6.3 While we are not yet consulting on applying the Duty to cryptoasset firms, we would like input on our options for securing broadly comparable outcomes for consumers in relation to regulated cryptoasset activities, ie, whether we should apply the Duty to all regulated cryptoasset activities with additional guidance or use tailored rules to achieve an appropriate standard of consumer protection for these activities.

6.4 When we previously consulted in CP25/14 (stablecoin issuance and crypto custody), a significant majority (80%) of respondents indicated that rules and guidance are required in addition to the Duty for stablecoin issuers, 83% agreed the same for qualifying cryptoasset custodians. We have proposed rules in addition to the Duty for other cryptoasset regulated activities in DP25/1 (cryptoasset activities). Proposed rules published to date do not cover all aspects of the Duty and we welcome views on whether applying the Duty or further tailored rules are required.

6.5 Principle 12 and PRIN 2A set out our Consumer Duty rules and guidance (with further guidance provided in FG22/5). The Duty comprises of:

6.6 **A consumer principle.** Principle 12 sets out that firms must act to deliver good outcomes for retail customers.

6.7 **3 cross-cutting obligations**, which set out high-level standards of behaviour:

- A firm must **act in good faith** towards retail customers.
- A firm must **avoid causing foreseeable harm** to retail customers.
- A firm must **enable and support retail customers** to pursue their financial objectives.

6.8 **4 sets of outcome rules** setting more detailed requirements and expectations in the following areas:

- **Products and Services** – products and services must be designed to meet the needs, characteristics and objectives of retail customers in an identified target market and distributed appropriately.
- **Price and Value** – firms must ensure products and services provide fair value to retail customers, and take appropriate action where they identify that this is not the case.
- **Consumer Understanding** – firms must communicate in a way that supports customers' understanding and equips them with the right information to make decisions that are effective, timely and properly informed.
- **Consumer Support** – firms must provide retail customers with the support they need throughout the lifecycle of the product or service.

Applying the Consumer Duty to cryptoassets and regulated cryptoasset activities

6.9 We want to ensure appropriate protection and secure outcomes for consumers in relation to cryptoasset activities, however, we are aware (for the reasons explained below) that achieving this faces specific challenges due to the nature of cryptoassets. This paper broadly explores 2 options:

6.10 **Option 1:** To apply the Duty, supplemented by sector-specific guidance where needed, or

6.11 **Option 2:** Not to apply the Duty, but to introduce rules that would achieve an appropriate standard of consumer protection for regulated cryptoasset activities.

6.12 These two broad options can be further sub-divided in relation to the type of cryptoasset recognising that aspects of the Duty better align with certain types of cryptoassets (eg UK issued qualifying stablecoins) than others.

Actionability of the Duty

6.13 The Duty does not give a private right of action (PROA) to retail customers. So, if the Duty is to apply, customers will not be able to bring court proceedings against a cryptoasset firm that causes a loss through a breach of the Duty.

Benefits of applying the Consumer Duty

6.14 Applying the Duty would help ensure consistent high standards for retail customers across financial services. Our 2025-30 Strategy sets out that the Duty is integral to how regulated financial firms treat their customers. We want to secure broadly comparable standards for customers engaging with cryptoasset firms. A benefit of the Duty is it allows the flexibility for sector-specific guidance, where required.

6.15 Applying the Duty would provide a baseline of consumer protections which ensures that cryptoasset firms, like other regulated firms, consider the needs and outcomes of their customers at every stage of the product or service lifecycle. Firms must apply the Duty in a way that's reasonable and reflects their size, role, and the risk their products pose to consumers. It would instil a consumer-centric mindset across a novel and fast evolving sector and ensure that firms consider the diverse needs of their customers, including those with characteristics of vulnerability.

6.16 The Duty's requirements on consumer understanding could be particularly helpful to ensure that consumers receive clear, fair and not misleading information, and are equipped to make decisions that are effective, timely and properly informed. These protections could be especially important in the cryptoasset sector, where risks and complexity can easily overwhelm retail investors.

6.17 While the cryptoasset sector thrives on innovation, it also needs clear boundaries to prevent abuse and ensure appropriate consumer protection. The Duty provides a framework that encourages responsible innovation. Firms can develop new products and services but must do so with a clear focus on delivering good outcomes for consumers.

6.18 The cryptoasset sector is fast evolving. The Duty has been designed to be outcome-focused, so would give cryptoasset firms flexibility to assess their customers' needs and tailor their products and communications accordingly. It is important to note that the Duty allows for more flexibility than prescriptive rules, which may constrain innovation or fail to keep pace with sector developments. The Duty is not a one-size-fits-all framework, and its flexible nature helps avoid inadvertently creating barriers.

Application to similar activities

6.19 The Duty already applies to authorised firms operating in the retail market (and will apply in the future to other authorised firms in respect of activities that relate to qualifying cryptoassets):

- Authorised firms communicating or approving financial promotions for qualifying cryptoassets.
- Authorised firms offering cryptoasset exchange traded notes to retail customers from October 2025.
- The Duty also applies to other high-risk investments made available to some retail consumers in traditional finance.

The case for not applying the Duty, but to introduce rules

6.20 The cryptoasset market is rapidly developing, and there are firms that want to seek authorisation under the new regime who have not previously been regulated.

6.21 The Duty is high level and may be challenging for some cryptoasset firms to interpret even if supplemented with guidance, to clarify how the Duty applies to cryptoasset activities.

6.22 Alternatively, additional rules tailored to the sector may be necessary to accommodate the specifics of this market and ensure rules are put in place in areas where we think they are most needed and have clear sectoral relevance.

6.23 For example, this could include rules around how firms communicate with and support consumers to ensure they can make informed decisions. Tailored product and service governance requirements could also add to consumer protections in a way that focuses on the role of FCA-authorised firms.

6.24 This alternative approach would arguably make standards of firms and consumers' understanding of firms' obligations to them clearer via more sector-relevant rules.

6.25 We can also see that certain requirements in PRIN 2A may not fit well with the cryptoasset sector, for example those relating to product governance (which assume there are known manufacturers), fair value, and avoiding causing foreseeable harm. These requirements may be more challenging to interpret and implement in the context of the cryptoassets market (as explored further below).

Challenges of applying the Consumer Duty

6.26 While there are various benefits in applying the Duty to the cryptoasset sector, we understand there are also several challenges.

Product governance – no clear issuer

6.27 Many cryptoassets, such as Bitcoin, are created and distributed by decentralised networks or unknown (anonymous) issuers that do not involve a firm and sometimes do not involve any known manufacturer at all. This could make it difficult or impossible for distributor firms to comply with product governance obligations that rely on at least some information being provided by the manufacturer. For qualifying cryptoassets issued by a UK-authorised firm, such as qualifying cryptoassets, where there is a clear issuer this challenge may not apply.

Product governance – target market

6.28 Under the Products and Services outcome of the Duty, a product manufacturer must identify a target market of customers for whom a product or service is designed and develop an appropriate distribution strategy. Distributors must then ensure that the product is distributed in line with the target market (see PRIN 2A.3 and Chapter 6 of FG22/5 (non-Handbook Guidance for firms on the Consumer Duty) for more information).

6.29 This may be difficult to implement in the cryptoasset context and may require significant changes or likely guidance relating to the Duty. Currently, cryptoassets are often issued without clear oversight or distribution controls. Absent an identifiable manufacturer who has developed a cryptoasset for a target market, compliance with requirements relating to the distribution of products may be difficult in practice. The fungible nature of cryptoassets is such that distributors will not have control over onward distribution of an

asset by third parties. This means those who create or promote the assets have limited ability to restrict who can access or buy them.

Price and value

6.30 If the Duty was applied in relation to regulated cryptoasset activities, cryptoasset firms would need to ensure that the cryptoassets and all services related to these assets provide fair value to retail customers. In this section when we refer to fair value we are referring to the reasonable relationship between the amount paid by a customer for the product or service and the benefits they can reasonably expect to get from it. The value of the asset is only one part of the fair value assessment.

6.31 It may be challenging to assess fair value under the obligations relating to price and value under the Duty given the high volatility and lack of inherent value of most cryptoassets. The price of the asset and the firm's charges (where based on the asset price) can vary significantly from one day to the next and bear an unclear relationship to an identifiable benefit to the consumer. In such cases, consideration of non-financial benefits alongside financial benefits may support a robust assessment of value. Similarly, firms should assess the financial and non-financial cost including where these may vary if, for example, based on the asset value.

6.32 Firms that distribute cryptoassets, such as unbacked cryptoassets like Bitcoin, would need to ensure that their own charges for distributing the asset represent fair value, and that the distribution arrangements do not result in the product ceasing to provide fair value for retail customers. If a product or service does not provide or ceases to provide fair value to customers, firms must take appropriate action to mitigate and prevent harm, for example, by amending it to improve its value, withdrawing it from sale, or where customers have suffered harm, providing redress. See PRIN 2A.4.27R and Chapter 7 of FG22/5 for more detail.

6.33 Where cryptoasset products are backed by assets that have an underlying value, such as qualifying stablecoins, the price is likely to be more stable. In such a situation it may be easier to conduct a fair value assessment. This assessment would more readily identify whether a product provides fair value and any relevant actions to take if it doesn't.

6.34 Where firms are charging fees for their services, we would expect authorised cryptoasset firms to account for the longer-term trends in asset price rises and falls in adjusting their fees and charges, particularly where they are a percentage of the underlying asset. It would likely not be fair value if an asset had risen in price steadily over the longer term and the firm kept its percentage-based charges the same, if the firm's operational costs for the activity or service remained relatively stable.

6.35 The price and value rules set out some specific features that fair value assessments should cover. There is also a non-exhaustive list of suggestions for further aspects that are useful to consider. These further aspects can be used to produce a robust fair value assessment that identifies whether or not customers will receive fair value, and any actions to take if they are not. One of these is benchmarking. In the cryptoasset market, firms might benefit from benchmarking their fees and charges against other firms offering cryptoasset loan products with a similar level of service provided to ensure their charges are not excessive. This benchmarking should be appropriately broad and not

targeted at a favourable subset of products or services. Our publication 'Price and Value Outcome: Good and Poor Practice update' is intended to help firms improve the way they think about fair value assessments.

6.36 We are interested in feedback from firms in how they assess and provide fair value for different cryptoassets.

Interaction with Admissions & Disclosures (A&D) regime

6.37 In DP24/4 (A&D and MARC), we asked whether respondents agreed with our view that while the Consumer Duty sets a robust baseline for expectations on firms, it is necessary to introduce specific A&D requirements to help support consumers.

6.38 Feedback from respondents to DP24/4 suggested broad interest in exploring whether bespoke A&D requirements could play a greater role in delivering consumer protection. Points raised included:

- While the Duty sets a baseline of expectations, respondents noted that bespoke A&D requirements could provide sector-specific granularity and relevance that consumers and market participants could benefit from.
- Bespoke A&D requirements could help ensure consumers are provided with the necessary information to make informed decisions, reducing uncertainty and compliance costs for firms.
- More tailored rules would support greater comparability and consistency across cryptoasset disclosures.

6.39 Having considered the feedback, we are inclined to the view that bespoke rules and guidance within the A&D regime would likely be an effective way to deliver an appropriate degree of consumer protection, focusing in particular on consumer understanding.

6.40 We are also considering whether applying the Consumer Duty rules directly to the A&D regime is appropriate, or whether bespoke rules and guidance could/would provide sufficient protection.

6.41 We welcome feedback on this consideration.

Next steps

6.42 Taking into account responses to CP25/14 (stablecoin issuance and crypto custody), as well as the importance of taking a consistent approach with traditional finance and other high-risk investments, we are proposing the Duty should apply to all regulated cryptoasset activities with additional guidance. Though we are seeking input as to whether this is the right approach or if tailored rules are more appropriate.

6.43 We see significant benefits in applying the comparable standards of consumer protection across all newly regulated cryptoasset activities and consider that not doing so could cause confusion for firms and consumers.

6.44 For clarity, we propose that we will not apply the Duty to the trading between participants of a UK authorised CATP. This is comparable to how we treat multilateral trading facilities (MTFs) in traditional finance. While CATPs will have much more direct retail access, we believe the proposed requirements and rules to be put in place will provide for non-discretionary, fair and transparent trading between all participants.

6.45 We expect that applying the Duty to the cryptoasset sector will instil a customer-centric mindset across all areas of business conduct and ensure that firms consider the diverse needs of their customers, including those with characteristics of vulnerability.

6.46 We will consider the responses to this discussion element before deciding our approach, which will be set out in a future CP.

6.47 Even if the Duty applies, most cryptoassets and associated products and services will remain high risk, speculative investments and consumers should be prepared to lose all their money if they buy them.

Question 13: **Do you consider that we should apply the Duty (along with additional sector-specific guidance)?**

Question 14: **Do you have views on where applying the Duty would be an effective way to achieve broadly comparable standards of consumer protection in the cryptoassets market, or where it might not?**

Question 15: **Do you consider that not applying the Duty, but introducing rules for regulated cryptoasset activities, would achieve an appropriate standard of consumer protection?**

Question 16: **If the Duty was not to apply, do you have views on what matters should be dealt with by sector-specific rules and guidance?**

Question 17: **Do you agree with our suggested approach under the A&D regime?**

Access to the Financial Ombudsman and the complaint handling rules

6.48 In this section, we invite discussion on whether customers should be able to bring complaints to the Financial Ombudsman when the firm has been unable to resolve the complaint and whether our complaint handling rules should apply to regulated cryptoasset activities.

6.49 We will consult on the outcome of this discussion in a follow up consultation.

6.50 The Financial Services and Compensation Scheme (FSCS) is the UK's statutory compensation scheme of last resort. The FSCS provides compensation to eligible complainants when a firm fails. In DP23/4, we outlined that we did not think we should extend FSCS protection to the newly regulated cryptoasset activities, but we will consider this further and consult in a future consultation.

Applying the DISP 1 Complaints Handling rules

6.51 The complaints handling rules in **Dispute Resolution: Complaints Sourcebook** chapter 1 set out rules and guidance on how firms should deal with customer complaints arising from regulated activities, including:

- the information firms must provide about their complaints handling process,
- the processes and procedures firms must have in place to assess a complaint,
- the time limits for dealing with complaints,
- and how firms must report on the complaints they receive.

6.52 The purpose of these rules is to ensure complaints between eligible complainants and firms are resolved quickly and effectively, providing fair and predictable redress outcomes when things go wrong, as well as contributing to a regulatory environment in which firms can compete, grow and invest for the long term.

6.53 We are currently considering applying the DISP 1 rules to all cryptoasset regulated activities, to ensure that customers who complain to their firm, for example, about harm arising from a lack of appropriate disclosures, have their complaints dealt with fairly. We are considering consulting on the application of the Financial Ombudsman Service and of the Dispute Resolution: Complaints Sourcebook (DISP) in a future CP largely premised on the possibility of a complaint received by a firm being referred to the Financial Ombudsman. The complaint handling rules in DISP 1 are interconnected with the DISP rules that outline the circumstances in which a complaint can be referred to the Financial Ombudsman (DISP 2) and then determined (DISP 3), for instance to account for the requirement to consider complaints 'fairly' and to take account of relevant FOS decisions or to communicate information on access to FOS's services.

6.54 Therefore, if we decide to apply the complaint handling rules (DISP 1), but do not wish to provide access to the Financial Ombudsman (as set out in DISP 2 and 3), we may need amendments to the complaint handling rules in DISP 1 to clarify how we expect them to resolve complaints in circumstances where there is no right to refer the complaint to the FOS.

6.55 We intend to consult on this position later this year, after we have finalised our position on access to the Financial Ombudsman.

About the Financial Ombudsman

6.56 In most circumstances, customers of retail financial services can refer complaints about regulated firms to the Financial Ombudsman if they are not satisfactorily resolved between customers and firms. The Financial Ombudsman is a free and informal alternative to courts for complaints' resolution which eligible complainants, as defined by DISP 2.7.3, can access. Access to the Financial Ombudsman encourages consumer confidence in the financial system.

6.57 The Financial Ombudsman can consider complaints which fall within either its compulsory jurisdiction (CJ) or voluntary jurisdiction (VJ). The CJ covers complaints relating to regulated activities as well as other specified financial activities and we have the power to decide what new activities should be covered by the CJ. The VJ rules are made by the Financial Ombudsman and covers firms not covered by the CJ carrying out activities which could be or are covered by the CJ. Firms can agree to join the VJ, by signing up to standard terms with the Financial Ombudsman.

6.58 The majority of cryptoassets will remain high risk, speculative investments and consumers should be prepared to lose all their money if they buy them. The Financial Ombudsman will not typically uphold complaints where the consumer complains about investment losses from poor performance of their investment. Instead, the Financial Ombudsman will decide on complaints based on what is fair and reasonable in all the circumstances of a case, and will take account of the relevant law, regulations and guidance as well as codes of practice or good industry practice.

Benefits of access to the Financial Ombudsman

6.59 In DP23/4 (stablecoins), we proposed extending the compulsory jurisdiction of the Financial Ombudsman to include complaints about regulated stablecoin issuers and custodians. We noted that access to an independent dispute resolution scheme increases trust and confidence in financial markets. Key reasons for supporting the proposals were:

- a.** Consumers currently understand the Financial Ombudsman, so it will be more easily adopted
- b.** The Financial Ombudsman is a well-established dispute resolution service
- c.** This approach provides consistency with other similar regulated activities.

6.60 Currently complaints about payment services and other regulated activities carried out by authorised firms are generally covered by the Financial Ombudsman. In the new regime, it may be beneficial to ensure consistency where customers engage with firms that are authorised to conduct both cryptoasset and traditional finance activities. Customers may find it easier to navigate complaints procedures when they can refer complaints about all firm activities to the Financial Ombudsman rather than just a sub-set.

6.61 Lastly, access to the Financial Ombudsman is available even where a complaint does not allege a breach which entitles them to damages claims in court. This means that, for example, a complaint based on a breach of the Consumer Duty could be dealt with by the Financial Ombudsman, even if it cannot give rise to a claim in court.

Further issues to consider regarding access to the Financial Ombudsman

6.62 We have identified several issues which would benefit from further consideration, and we welcome views on how to address them.

6.63 **Overseas firms:** The Financial Ombudsman's Compulsory Jurisdiction (CJ) predominantly covers activities carried on from an establishment in the United Kingdom (and complaints relating to these). The Financial Ombudsman Service may choose to extend the Voluntary

Jurisdiction (VJ) for those activities that are not in scope of the compulsory jurisdiction, but it is up to the firm if they agree to join the VJ. Some cryptoasset firms may be based outside of the UK and therefore UK customers may be served by overseas firms. In these cases, customers may not be able to bring complaints against these overseas firms to the Financial Ombudsman unless the Financial Ombudsman extends its VJ (and the overseas firms opt in). This means customers of overseas cryptoasset firms may find it difficult to understand what consumer protections apply to them, particularly for access to the Financial Ombudsman. In principle, this could be mitigated by placing disclosure requirements on overseas firms to ensure their customers know they cannot refer complaints to the Financial Ombudsman.

6.64 Third party firms: Generally, to bring a complaint to the Financial Ombudsman, a complainant must have an eligible relationship with the authorised firm. In some instances, a third-party firm may act on behalf of an authorised firm. Our understanding is that this third-party arrangement may exist for stablecoin issuers. There is a risk that customers may not be clear when they can refer a complaint to the Financial Ombudsman when there is a third party acting on behalf of an authorised firm. This risk could be mitigated through a requirement that, where a stablecoin issuer contracts a third party to provide services on their behalf, they will require the third-party provider to make appropriate disclosures about how they can make a complaint and who to complain to. This risk could also be mitigated by **capturing the third party and the customer as an eligible relationship**.

6.65 International comparisons: We will take into account how far our approach on access to alternative dispute resolution aligns with other regimes. This will ensure that our approach remains competitive.

Next steps

6.66 Subject to feedback from these discussion questions, and the feedback previously received in [DP23/4](#), our current position is that we are likely to consult on the DISP 1 complaint handling rules and access to the Financial Ombudsman applying to all newly regulated cryptoasset activities. We are very interested to hear feedback on this position. We would also be particularly interested to hear whether there should be any exemptions for any of the newly regulated cryptoasset activities.

Question 18: **Should customers be able to refer complaints relating to cryptoasset activities to the Financial Ombudsman?**

Question 19: **Are there any additional factors that we should take into account when considering if it is appropriate for the Financial Ombudsman to consider complaints about cryptoasset activities (eg complaints where a firm is based overseas or where a third party is acting on behalf of an authorised firm)?**

Question 20: **Are there specific activities the Financial Ombudsman should not be able to consider complaints for? Please explain.**

Chapter 7

Discussion Chapter – Conduct of Business Sourcebook and Product Intervention and Product Governance Sourcebook

7.1 This chapter contains a discussion on our proposed approach to the Conduct of Business Sourcebook (COBS) and Product Intervention and Product Governance Sourcebook (PROD) to cryptoassets firms.

7.2 Both COBS and PROD sections should be read alongside the Consumer Duty chapter as they share many of its intended outcomes. Together, they form part of a holistic framework for consumer protection. We will seek to consult on these topics by the beginning of next year.

Overall approach

7.3 We are seeking feedback on whether and how COBS should apply to cryptoasset firms offering future cryptoasset regulated activities, as well as our proposed approach to product governance. We also consider whether and when reliance on the Consumer Duty may be appropriate instead of applying PROD or aspects of COBS.

Conduct of Business Sourcebook (COBS)

Overview of the current framework

7.4 COBS rules require firms to act honestly, fairly and professionally in accordance with the best interests of their client. Firms must also communicate in a clear, fair, and not misleading way. The goal is to help clients understand key risks and their level of protection, enabling informed decisions. The only part of COBS that currently applies is our financial promotion requirements which have been in place since October 2023. Apart from rules on financial promotions, there are no conduct of business requirements for cryptoasset firms.

7.5 In considering how to apply COBS to cryptoasset firms, our aim is to ensure consumer protection, transparency, market integrity, and fair treatment of clients.

Stakeholder feedback

7.6 Our proposals reflect feedback from previous discussion and consultation papers. In DP23/4 (stablecoins), we explored whether application of COBS should apply to regulated stablecoin issuers and custodians. Around 60% of respondents supported this, citing the risks of stablecoins and the need for a potential tailored approach.

7.7 In CP25/14 (stablecoin issuance and crypto custody), we consulted on bespoke conduct rules for stablecoin issuers and cryptoasset custodians, reflecting their distinct business models and potential systemic impact. Proposals included requirements for contractual relationships with holders and third-party agreements. Most respondents supported these rules, highlighting the technical complexity of cryptoassets and the value of clear, tailored standards in a newly regulated sector.

Vulnerabilities and risks in the sector

7.8 Evidence from past failures in the cryptoasset market shows that poor conduct standards have significantly contributed to consumer harm. Some firms failed to disclose key risks about complex activities like asset rehypothecation and lending, while others hid conflicts of interest or made misleading claims about the firm insurance cover. These cases underscore the need for a strong conduct framework for regulated cryptoassets firms.

7.9 In August 2024, we published 'Good and poor practice: Assessing firms' compliance with 'back end' cryptoasset financial promotion rules', noting that many assessments missed topics outlined in COBS 10 Annex 4G. Our FG23/3 (financial promotions guidance) clarified that firms should address all 12 matters listed in the annex. We observed widespread non-compliance, with firms allowing consumers to invest in cryptoassets despite failing appropriateness assessments. This exposed consumers to harm, especially when they don't fully understand the nature or risks of the cryptoassets being promoted.

Summary of proposals

7.10 As outlined in Chapter 1, and subject to consultation feedback, we are proposing to extend our Handbook glossary definition of 'designated investment business' (DIB) to include the future cryptoasset regulated activities under the new regime which are highlighted in paragraph 1.2.

7.11 Consequently, various COBS requirements applying to firms' DIBs would apply to these firms. The table below illustrates how COBS could be applied. COBS requirements will be part of the matrix of conduct rules on firms. Below we give a high-level illustration of what these requirements are. The intent is that COBS requirements will be supplemented by bespoke rules for the new cryptoasset regulated activities.

Handbook	Summary of areas and rationale
COBS 1 Application; COBS 2 Conduct of business obligations; COBS 3 Client categorisation; COBS 6 Information about the firm, its services and remuneration COBS 10 Appropriateness COBS 16 Reporting information to clients (non-MiFID provisions)	<p>We are considering applying these chapters generally to cryptoasset firms, with some exceptions or adjustments. We consider exceptions and adjustments necessary as those provisions either refer to types of firms in traditional financial services that do not have equivalent or similar risks compared to cryptoasset activities (eg MiFID, insurance, pensions):</p> <ul style="list-style-type: none"> • COBS 1: applying only 1.1, 1.2 and Annex 1; amending Annex 1 with a carve out for transactions between CATPs and professional clients as they are afforded a lighter level of protection due to their knowledge and skills. • COBS 2: applying 2.1, 2.2, 2.3, 2.4, 2.5. • COBS 3: applying all provisions except 3.7, subject to broader consultation on client categorisation. • COBS 6: applying only 6.1. • COBS 10: applying this entire chapter; amending Annex 4G. • COBS 16: applying 16.1 and 16.4, with amendments to 16.4 to capture "qualifying cryptoassets".
COBS 4 Communicating with clients, including financial promotions; COBS 8 Client agreements (non-MiFID provisions)	<p>We propose to apply these provisions to cryptoassets firms with some changes to how UK issued qualifying stablecoins are treated.</p>
COBS 11 Dealing and managing; COBS 13 Preparing product information; COBS 14 Providing product information to clients	<p>We are considering applying these requirements for specific cryptoasset regulated activities, and plan to consult on this in our future CP.</p>

7.12 We are proposing to not apply the following COBS chapters to the activities of cryptoasset firms:

7.13 COBS 5 Distance communications; COBS 7 Insurance distribution; COBS 10A Appropriateness (for non-advised services) (MiFID and insurance-based investment products provisions); COBS 12 Investment Research; COBS 15 Cancellation; COBS 16A Reporting information to clients (MiFID and insurance-based investment products provisions); COBS 17 Claims handling for long-term care insurance; COBS 18 Specialist Regimes; COBS 19 Pensions supplementary provisions; COBS 20 With-profits; COBS 21 Permitted Links and conditional permitted links; COBS 22 Restrictions on the distribution of certain investment products.

7.14 We are not proposing to apply these chapters of COBS because they cover:

- Activities or market activities that do not have a cryptoasset-equivalent;
- Methods of distance communication that do not reflect the current development of technology as well as current marketing practices; or
- focus on MiFiD firms.

Applying our conduct standards to the activities of authorised cryptoasset firms

COBS 1 – Application

7.15 COBS 1 is the general application provision, setting out the scope of the sourcebook.

7.16 We are considering applying COBS to cryptoassets firms in a way that aligns with how COBS currently applies to FSMA-authorised firms, with some adaptations, for example, COBS rules will apply for transactions between Cryptoasset Trading Platforms (CATPs) and retail clients, but not for those transactions between CATPs and professional clients. As regards the application of COBS to CATP operators, acting in that capacity, and transactions on CATPs, we are considering an approach comparable to the operation of an MTF (see COBS 1 Annex 1) but which has regard the fact there is likely to be a material number of retail investors trading on the platform. As such, whilst much of COBS will be disapplied for professional investors as regards the CATP's services to them, COBS protections should be applied as regards the CATP operator's services to retail investors.

COBS 2 – Conduct of Business obligations

7.17 COBS 2 outlines firms' core obligations, including fair treatment of clients, managing conflicts of interest, and making appropriate disclosures.

7.18 Firms must act honestly, fairly, and professionally, providing timely and accurate disclosures. Applying COBS 2 means firms must avoid misleading claims, for example, overstating financial health or regulatory approval.

7.19 Cryptoasset firms will be required to provide clear, fair and non-misleading information before offering services. This includes disclosures about the firm, its services, designated investments, proposed strategies, execution venues, and all relevant costs and charges, along with appropriate risk warnings.

COBS 3 – Client Categorisation

7.20 We are considering applying client categorisation rules in COBS 3 to cryptoasset firms.

7.21 Under COBS 3 firms must categorise clients as retail, professional, or ECPs. Different types of clients generally have different levels of protection, with retail clients generally receiving the highest level of protection. Professional clients, who typically have higher level of knowledge, expertise and experience, have less protection but are still covered by some rules such as those on communication and financial promotions. ECPs receive the least protection, with many COBS rules not applying to them.

7.22 Following industry feedback from CP24/24 (MiFID Organisational Regulation), we plan to consult on changes to the client categorisation rules in the near future. The future consultation on COBS 3 will also be relevant to cryptoassets firms as it will include proposals on when a client can request re-categorisation. Changes to the Handbook regarding client categorisation will apply across all Firms.

COBS 4 – Communicating with clients, including financial promotions

7.23 The Financial Promotion regime for qualifying cryptoassets came into force in October 2023. Since then, firms communicating qualifying cryptoasset financial promotions must comply with our rules. We published guidance to help firms comply with the regime in November 2023. We have taken action where firms have not met our standards ensuring that the promotions have been amended or withdrawn. In 2024 19,766 promotions were amended or withdrawn by firms communicating promotions, of these 1,098 were related to cryptoassets.

7.24 Under the draft RAO SI, new cryptoasset activities, and any related promotions, will fall under the existing financial promotions regime as promotions related to qualifying cryptoassets. Currently, qualifying cryptoassets are classified as Restricted Mass Market Investments (RMII). Marketing restrictions for RMII include conditions such as appropriateness assessments, a 24-hour cooling-off period for new customers, appropriate client categorisation and prominent risk warning.

7.25 We are considering whether we should reclassify the RMII status for UK-issued qualifying stablecoins, which would mean that they would not be subject to marketing restrictions. They would still be subject to other general financial promotion requirements, such as the fair, clear and not misleading rule. This reflects their comparatively lower risk profile relative to other cryptoassets. Additionally, the reclassification would assist future use cases for UK-issued qualifying stablecoins, for example for retail payments.

7.26 To help consumer understanding, we are considering whether financial promotions for qualifying stablecoins not issued by a UK-authorised issuer should include additional risk warning information. This would tell consumers when a stablecoin is issued outside the UK or by a non-authorised firm.

7.27 Proposed application of COBS 4 for risk warnings

Cryptoasset	Existing or proposed warning	Nature of risk warning
UK-issued qualifying stablecoins	Proposed	No risk warning, still subject to other financial promotion requirements such as the fair, clear and not misleading rule.
Qualifying Cryptoasset	Existing warning (COBS 4.12A11 (1D) R)	Don't invest unless you're prepared to lose all the money you invest. This is a high-risk investment and you should not expect to be protected if something goes wrong.

Cryptoasset	Existing or proposed warning	Nature of risk warning
Qualifying stablecoins not issued by a UK-authorised qualifying stablecoin issuer	Proposed with additional content in bold	The issuance of this stablecoin is not regulated in the UK. Don't invest unless you're prepared to lose all the money you invest. This is a high-risk investment and you should not expect to be protected if something goes wrong.

Question 21: **Do you agree with our proposal that UK-issued qualifying stablecoins should not be classified as Restricted Mass Market Investment (RMMI), which will not be subject to marketing restrictions? Why/Why not?**

Question 22: **Do you agree with our proposal that financial promotions for qualifying stablecoins not issued by an FCA-authorised UK issuer should include additional risk warning information? Why/Why not?**

COBS 5 – Distance Communication

7.28 COBS 5 sets out the rules firms must follow when marketing their products to consumers from a geographical distance.

7.29 This chapter is based on the Directive of the Council and Parliament of 23 September 2002 on distance marketing of consumer financial services (No 2002/65/EC) (DMD) and the language used throughout the chapter does not reflect how cryptoasset firms conduct their distance marketing activities (eg through telephone). We are therefore considering not applying COBS 5. The discussion in Chapter 6 on the Duty is related to this proposal, and we welcome feedback on whether relying on the Duty and additional guidance is sufficient to achieve clear distance communications for cryptoassets.

Question 23: **Do you agree that applying the Duty and additional guidance would be sufficient to achieve clear distance communications for cryptoassets or whether we should consider more specific rules such as those set out in COBS 5?**

COBS 6 – Information about the firm, its services and remuneration

7.30 COBS 6 covers firm and compensation disclosures. As noted earlier, we do not propose applying provisions designed for MiFID businesses, which differ significantly from cryptoasset activities in nature and risk. In line with our strategic outcome of supporting consumers and the rule to act in clients' best interests, firms must consider how and when they provide relevant information. Cryptoasset firms should ensure timely, appropriate communication through suitable channels to help clients make informed decisions.

7.31 We are considering applying COBS 6 to require cryptoasset firms to disclose information about the firm and its services. This includes details on registered status, conflict of interest policies, and the nature, frequency, and timing of performance reports.

7.32 These disclosures are given to existing clients and specifically cover safeguarding client assets and money. We are also considering requiring firms that hold client money or qualifying cryptoassets to inform clients about safeguarding arrangements, including third-party involvement and responsibility in case of issues affecting assets or funds.

COBS 8 – Client agreements (non-MiFID provisions)

7.33 We are considering applying COBS 8 in full. This will require cryptoasset firms to give clients their client agreements before they are bound by them. The agreement must be provided in a durable medium and must cover the terms and conditions of the agreement and information about the firm and its services. We are also considering that cryptoassets firms must notify clients in good time about any material change to the information given in the client agreement.

COBS 10 – Appropriateness (for non-advised services) (non-MiFID and non-insurance-based investment products provisions)

7.34 COBS 4.12A.28R requires that where a firm or person is aware, or ought to be aware, that an application or order to transact in qualifying cryptoassets is in response to a direct order financial promotion they must only process that application or order once it has assessed that the qualifying cryptoasset is appropriate for the retail client in compliance with the rules in COBS 10. This obligation applies to all firms that communicate or approve financial promotions of cryptoassets to UK consumers.

7.35 That appropriateness assessment should evaluate whether the consumer has sufficient knowledge and experience of the service or product being promoted. Typically, this is conducted through an interactive online questionnaire, often without direct human involvement. However, the firm remains responsible for ensuring that they are satisfied that this assessment meets our requirements.

7.36 Our publications PS23/6 (cryptoasset financial promotion rules) and FG23/3 (financial promotions guidance) give more detail on our expectations.

7.37 As set out in the financial promotions guidance, authorised cryptoasset firms should consider whether they need to include additional or alternative questions to reflect the specific nature and risks of the cryptoasset product or service being promoted.

7.38 We want firms communicating and approving financial promotions for cryptoassets to design robust assessments that effectively test consumers' understanding of relevant risks and experience. COBS 10 Annex 4G provides guidance on designing robust assessments, but there are no specific rules that require certain matters to be included in the design of the appropriateness test.

7.39 In August 2024 we published our 'Good and poor practice: Assessing firms' compliance with 'back end' cryptoasset financial promotion rules'. This included observations that many firms' assessments did not cover all relevant topics outlined in COBS 10 Annex 4G. We also saw that most firms will allow consumers to invest in specific cryptoasset products despite the outcome of the appropriateness assessment.

7.40 These findings suggest that many firms are not designing assessments that adequately reflect our expectations. To address this, we are considering changing COBS 10 Annex 4G from a guidance provision to a rule. This would require firms to design questions for the appropriateness test covering all the matters currently set out in COBS 10 Annex 4G. This will better ensure that firms are complying with our rules allowing us to reduce harm to consumers by taking action quicker.

7.41 Firms would still be able to include additional questions where necessary to reflect the specific risks of the cryptoasset product or service being promoted.

7.42 We also intend to consult on other appropriateness test obligations for activity specific products as part of our future CPs.

Question 24: Do you agree with our overall approach to the appropriateness test? Are all 12 matters in COBS 10 Annex 4G relevant? Why, why not?

COBS 11 – Dealing and Managing

7.43 We are proposing to consult on best execution rules in our future CP.

COBS 13 and 14 – Preparing product information and providing product information to clients.

7.44 COBS 13 and COBS 14 require firms to prepare and deliver product information that helps clients understand key product features. COBS 13 sets standards for disclosing information on packaged products, such as life policies, CIS, and pension schemes, including objectives, risks, charges, and cancellation rights. COBS 14 outlines how and when firms must deliver this information before clients are bound by a contract. Given the complexity and variety of cryptoasset products, we believe COBS 13 and 14 are insufficient. We will consult on tailored conduct requirements for product information in our future CP.

COBS 15 – Cancellation

7.45 COBS 15 outlines rules on contract cancellation, including cooling-off periods and firm obligations when a client exercises this right. It also includes an annex listing products exempt from cancellation rights. COBS 15 Annex 1 exempts distance contracts whose price depends on market fluctuations beyond the firm's control. Cryptoassets are highly volatile, and our consumer guidance has consistently warned that investors should be prepared to lose all their money. Though price movements in cryptoassets are outside firms' control. Given this, we do not plan to consult on cancellation rights for cryptoasset services and products.

7.46 This approach aligns with existing rules for other financial instruments like futures and options, which are also exempt due to market-driven price fluctuations. Offering cancellation rights in these cases would unfairly burden firms.

Question 25: Do you think there should be cancellation rights for distance contracts related to cryptoassets products or activities whose price is not driven by market fluctuation such as staking and safeguarding?

COBS 16 – Reporting information to clients. (non-MiFiD provisions)

7.47 COBS 16 sets out client reporting rules, requiring firms to provide regular statements on client assets and money to keep clients informed about value and custody arrangements.

7.48 As noted in the previous chapter, we are considering specific information cryptoasset firms should provide about qualifying cryptoassets and client money. We also plan to consult on product information requirements in our future CP.

7.49 As part of COBS 16.4, we are considering requiring firms holding qualifying cryptoassets or client money to issue periodic statements with key information, such as up-to-date valuations. This would also apply to firms offering staking, lending, or borrowing. Statements must be provided at least annually in a durable medium, unless clients have online access and have viewed a current statement within the past quarter.

7.50 We do not consider COBS 16.2 (occasional reporting) and 16.3 (periodic reports for managed investments) to be broadly applicable to cryptoasset activities. These may duplicate disclosure rules already consulted on in CP25/14 (stablecoin issuance and cryptoasset custody). We are therefore considering consulting on these provisions and their annexes (1R and 2R) in our future CP.

Question 26: Do you agree with our overall approach to Conduct of Business requirements? If not, why not?

Product Intervention and Governance

7.51 PROD focuses on strengthening firms' product oversight and governance. It requires systems and controls for designing, approving, marketing, and managing products throughout their lifecycle. The purpose of the PROD rules are to achieve good product governance that should result in products that: meet the needs of one or more identifiable target markets; are sold to clients in the target markets by appropriate distribution channels; and deliver appropriate client outcomes.

Desired outcomes

7.52 We have seen harm occur in the cryptoasset sector when products or services were poorly designed or widely distributed to customers for whom they were unsuitable.

Under our new regime, we expect authorised cryptoasset firms – whether acting as manufacturers or distributors – to maintain effective governance throughout the product and service lifecycle. In particular, we want to ensure these products and services are designed and distributed to meet the needs of their target market. By 'target market', we mean one or more groups sharing common features whose characteristics, needs and objectives the product or service is, or will be, designed to address. However, given the complexities of identifying a target market for crypto products and services, set out at earlier in the chapter, we would expect firms, particularly distributors of products manufactured by non-authorised cryptoasset firms, to ensure that firms consider the diverse needs of their customers, including those with characteristics of vulnerability. We set out our expectations for firms on the fair treatment of vulnerable customers in FG21/1 (Guidance for firms on the fair treatment of vulnerable customers).

Challenges with PROD

7.53 We have identified several challenges in applying the PROD framework to cryptoasset firms. If PROD were to apply to cryptoassets, the closest analogy would be the requirements in PROD 3 for MiFID instruments. Existing PROD chapters, such as PROD 3, require authorised manufacturers and distributors to establish systems and controls to design, approve, market and manage products throughout the product's lifecycle. In our Handbook, 'products' refer to specified investments which are distributed and any service which involves or includes the carrying on of a regulated or ancillary activity. As noted in Chapter 6, many cryptoassets, such as Bitcoin, are created and distributed by decentralised networks or anonymous issuers which makes it difficult to determine who regulatory obligations should apply to.

7.54 For certain cryptoassets, such as stablecoins, fungibility and transferability mean that products sold initially to non-retail customers can easily be sold on to a retail customer over the lifetime of the product. The provisions in PROD apply to both retail and non-retail customers this presents challenges in applying rules that we intend solely for retail markets, such as ensuring that products and services designed for non-retail customers are not accessed by retail customers.

Proposed approach to product governance

7.55 We are therefore considering not applying the existing PROD provisions, nor designing a new chapter in our PROD sourcebook for firms that provide cryptoasset products or services. In light of the discussion in Chapter 6, we welcome feedback on whether relying on the Duty and additional guidance is sufficient to achieve our intended product governance outcomes, or whether bespoke cryptoasset product and service governance rules or guidance is needed.

Question 27: Do you agree that applying the Duty and additional guidance would be sufficient to achieve adequate product governance for cryptoassets or should we consider more specific rules such as those set out in PROD?

Chapter 8

Next steps

- 8.1** To help firms and stakeholders understand the policy rationale and considerations of our proposals and to gather feedback, we will arrange a series of in-person and virtual engagements.
- 8.2** We welcome feedback on the impact of our policy proposals on business models, domestic and international market participants and the market. We also welcome suggestions on any other relevant market developments we have not considered or unintended consequences of our proposals.
- 8.3** For our discussion proposals in Chapters 6 to 7, we will take into account the feedback and suggestions received, and consult on detailed requirements (rules and guidance), alongside our other remaining consultations (such as activity-specific requirements) within our Crypto Roadmap throughout 2025-26.
- 8.4** For our consultation proposals in Chapters 2 to 5, we will consider the feedback and build those into our final rules as appropriate through Policy Statements. We will also provide further guidance to support firms transition from MLR registration to our FSMA authorisation regime, where they are in scope of the new regulated activities for cryptoassets. Our finalised rules will be set out in Policy Statements, which we intend to publish in 2026 as per our Crypto Roadmap.

Annex 1

Questions in this paper

Question 1: Do you agree that new cryptoasset activities defined in the SI (and as described as 'qualifying cryptoasset activities' in draft FCA Handbook rules) should fall under the category of 'designated investment business' for the purposes of applying relevant sections of the Handbook?

Question 2: Do you agree with our proposal for applying high level standards to cryptoasset firms in a similar way they apply to traditional finance?

Question 3: Do you agree with our proposed application of the existing SUP rules (except SUP 16) to cryptoasset firms?

Question 4: Do you agree with our proposal to require cryptoasset firms to follow the existing requirements in SYSC 1, 4 – 7, 9 – 10, and 18 in the same way as existing FCA-regulated firms (or existing DIBs)?

Question 5: Do you agree with our proposal to apply the existing SM&CR regime to cryptoasset firms, taking into account various parallel consultations on the broader SM&CR regime to ensure consistency? If not, please explain why.

Question 6: Do you agree with the proposed categorisation for enhanced cryptoasset firms, such as the threshold for allowing cryptoasset custodian firms to qualify as enhanced? Should we consider other ways to categorise cryptoassets firms as enhanced?

Question 7: Do you agree with our proposal to extend the application of SYSC 15A to cover all cryptoasset firms, including FSMA-authorised firms carrying out qualifying cryptoasset activities? If not, please explain why.

Question 8: Do you agree with our proposal that the use of permissionless DLTs by cryptoasset firms should not be treated as an outsourcing arrangement? If not, please explain why.

Question 9: Do you agree with our proposal to require cryptoasset firms to follow the same financial crime framework as FSMA-authorised firms? If not, please explain why.

Question 10: Do you agree with the guidance set out in this document, and can you outline any areas where you think our approach could be clearer or better tailored to the specific risks and business models in the cryptoasset sector?

Question 11: Are there any emerging digital and cyber security industry practices or measures which we should consider when supporting cryptoasset firms complying with operational resilience and related requirements? Please elaborate.

Question 12: Do you agree with our proposal to apply the ESG Sourcebook to cryptoasset firms?

Question 13: Do you consider that we should apply the Duty (along with additional sector-specific guidance)?

Question 14: Do you have views on where applying the Duty would be an effective way to achieve broadly comparable standards of consumer protection in the cryptoassets market, or where it might not?

Question 15: Do you consider that not applying the Duty, but introducing rules in the cryptoassets market would achieve an appropriate standard of consumer protection?

Question 16: If the Duty was not to apply, do you have views on what matters should be dealt with by sector-specific rules and guidance?

Question 17: Do you agree with our suggested approach under the A&D regime?

Question 18: Should customers be able to refer complaints relating to cryptoasset activities to the Financial Ombudsman?

Question 19: Are there any additional factors that we should take into account when considering if it is appropriate for the Financial Ombudsman to consider complaints about cryptoasset activities (eg complaints where a firm is based overseas or where a third party is acting on behalf of an authorised firm)?

Question 20: Are there specific activities the Financial Ombudsman should not be able to consider complaints for? Please explain.

Question 21: Do you agree with our proposal that UK-issued qualifying stablecoins should not be classified as Restricted Mass Market Investment (RMMI), which will not be subject to marketing restrictions? Why/Why not?

Question 22: Do you agree with our proposal that financial promotions for qualifying stablecoins not issued by an FCA-authorised UK issuer should include additional risk warning information? Why/Why not?

Question 23: Do you agree that applying the Duty and additional guidance would be sufficient to achieve clear distance communications for cryptoassets or whether we should consider more specific rules such as those set out in COBS 5?

Question 24: Do you agree with our overall approach to the appropriateness test? Are all 12 matters in COBS 10 Annex 4G relevant? Why, why not?

Question 25: Do you think there should be cancellation rights for distance contracts related to cryptoassets products or activities whose price is not driven by market fluctuation such as staking and safeguarding?

Question 26: Do you agree with our overall approach to Conduct of Business requirements? If not, why not?

Question 27: Do you agree that applying the Duty and additional guidance would be sufficient to achieve adequate product governance for cryptoassets or should we consider more specific rules such as those set out in PROD?

Question 28: Do you agree with our assumptions and findings as set out in this CBA on the relative costs and benefits of the proposals contained in this consultation paper? Please give your reasons.

Question 29: Do you have any views on the cost benefit analysis, including our analysis of costs and benefits to consumers, firms and the market?

Annex 2

Cost benefit analysis

Summary

- 1.** Cryptoassets are increasingly popular with UK consumers. Our Cryptoasset Consumer Research survey data indicates demand among UK adults has tripled since 2020 (from 4% to 12%), with consumers primarily motivated by large asset price rises and the potential opportunity to make money quickly.
- 2.** UK consumers typically purchase cryptoassets through large cryptoasset-specific trading platforms (mostly based overseas), or through UK brokerages and payment firms. Our research indicates UK consumers generally report positive experiences from engaging in cryptoasset markets.
- 3.** However, information asymmetry, behavioural distortions, and misaligned incentives, in addition to evolving and complex product features, can mean some consumers lack understanding of cryptoassets and their associated risks, or spend more than intended. This can result in excessive risk-taking, or consumers being exposed to financial crime, which is common in cryptoasset markets. Firms may face weak incentives to address these risks, due to limited regulatory oversight, and as doing so could potentially result in reduced profits.
- 4.** Our current regulatory remit for cryptoassets is limited to the Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), the financial promotions regime, and consumer protection legislation (including the Consumer Rights Act 2015 and Consumer Protection from Unfair Trading Regulations 2008).
- 5.** His Majesty's Treasury (the Treasury) recently published draft legislation to bring certain cryptoasset-related activities under our regulation. Firms will require authorisation by the FCA to conduct these activities in UK markets. Firms registered with us to undertake these activities will also be subject to FCA rules and guidance. We are proposing applying FCA Handbook rules to firms which are authorised to conduct regulated cryptoasset activities. These Handbook rules, which apply to most firms we regulate, establish minimum standards and levels of consumer protections within UK regulated financial markets.
- 6.** By applying these rules to firms undertaking cryptoasset regulated activities, we intend to create a level-playing field across cryptoasset and non-cryptoasset firms, in line with the design principle of "same risk, same regulatory outcome". We expect our intervention will create stronger incentives for cryptoasset firms to improve their conduct and accountability, raising standards across the sector, which we anticipate will result in reduced consumer harm.

7. This CBA assesses the impact of applying certain FCA Handbook rules and guidance, (including SYSC and PRIN) to cryptoasset firms. Our central present value estimate of total direct net benefits from our proposals over a 10 year appraisal period is £38m.
8. Benefits accrue to consumers through reduced harm from financial crime, in particular reduced frauds and scams. Other, non-quantified benefits include improved regulatory clarity to firms and consumers.
9. Costs are primarily driven by compliance familiarisation and business model changes that our regulation will introduce for firms. Firms will need to become familiar with FCA Handbook rules and guidance, and update their internal processes to become compliant, which will result in costs to them. Our breakeven analysis indicates our proposed intervention will be net beneficial if the net benefit experienced by each UK cryptoasset consumer exceeds £12 across our 10-year appraisal period.
10. Our regulation aims to change incentives to firms (which drive the benefits of our intervention) which may require significant changes to firm business models. Firms may pass on these costs to consumers, in the form of higher prices.

Summary of costs and benefits (10 years, present values, central estimates)

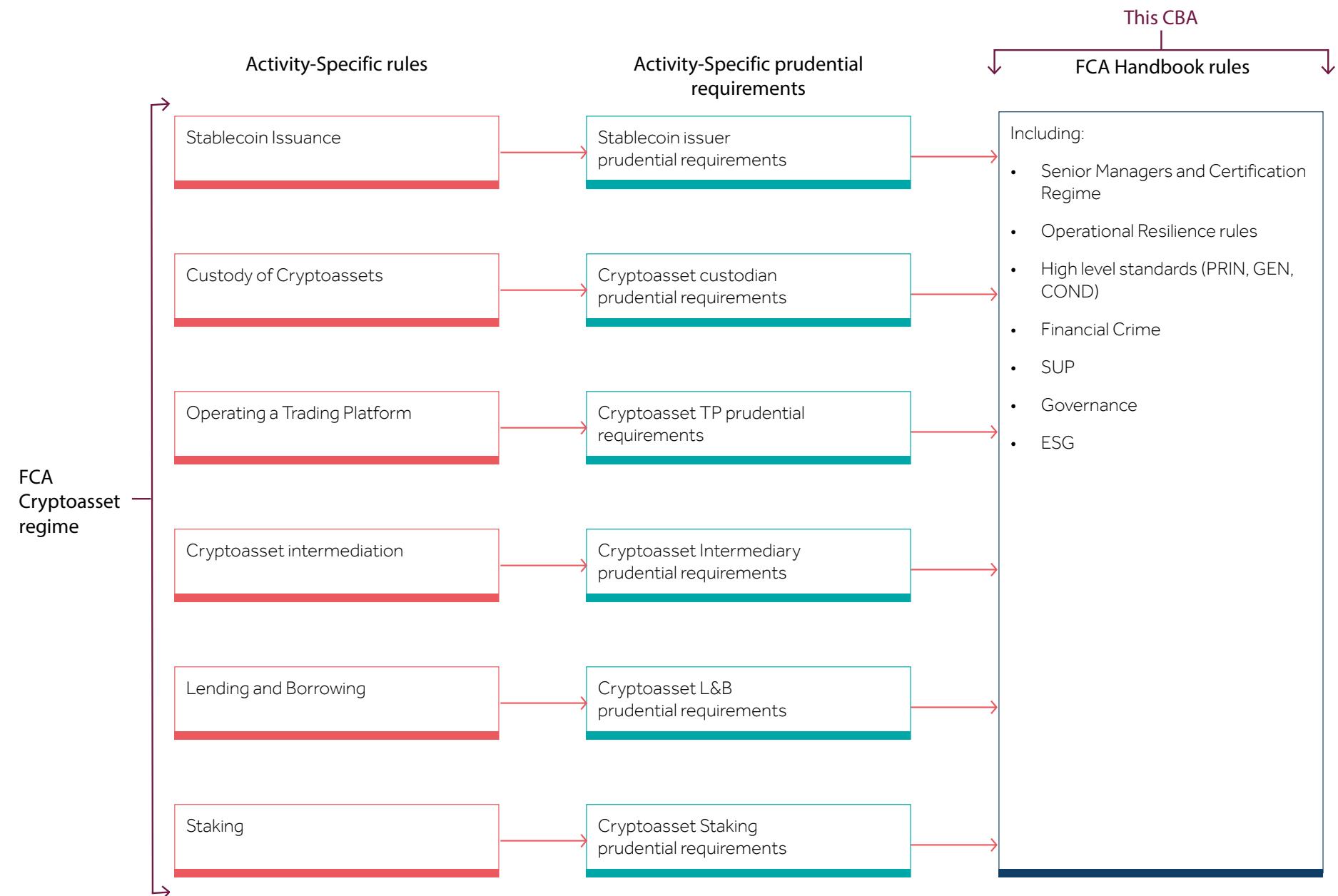
Group Affected	Item Description	PV Benefits	PV Costs
Firms	Firm Standards (SYSC)		
	<i>Senior Managers and Certification Regime</i>		£9.8m
	<i>Financial Crime rules</i>		£2.6m
	<i>Operational Resilience</i>		£39.1m
	Other Requirements		
	<i>High Level Standards</i>		£1.1m
	<i>Additional Custodian requirements</i>		£40.1m
Consumers	Reduced Losses from scams	£130m	
Total impacts		£130m	£92.6m
Net Impact			+£37m NPV

11. Overall, we anticipate applying FCA Handbook rules to cryptoasset firms to deliver significant net benefits and be proportionate. The proposed rules and guidance will introduce higher standards and improved protections for consumers who choose to engage in cryptoasset markets, the benefits of which we estimate as being more substantial than higher compliance costs to firms.

Introduction

- 12.** The Financial Services and Markets Act (2000) requires us to publish a cost benefit analysis (CBA) of our proposed rules. Specifically, section 138I requires us to publish a CBA, defined as 'an analysis of the costs, together with an analysis of the benefits that will arise if the proposed rules are made'.
- 13.** In the UK, cryptoassets are currently regulated for Anti-Money Laundering and Countering Terrorist Financing (AML & CTF). As of June 2025, there over 50 firms registered with the FCA for these purposes, as listed [here](#). Firms also must comply with the Travel rule and collect, verify and share transmit information about both the originator and beneficiary of a cryptoasset transfer. In addition, since October 2023, cryptoasset firms offering products to UK consumers must comply with our financial promotions' regime.
- 14.** As set out in draft legislation, the Treasury has proposed establishing a UK regulatory regime for cryptoassets and introducing several cryptoasset activities into our regulatory perimeter. Firms will also face prudential requirements associated with the cryptoasset activities they undertake and need to comply with rules relating to market abuse and admissions/ disclosures to clients.
- 15.** In addition to "activity-specific" rules and prudential requirements, we are proposing firms undertaking regulated cryptoasset activities be subject to wider FCA Handbook rules and standards, in the same way as other FSMA authorised firms. An illustration of how we anticipate firms to be affected by the scope of our proposed rules is set out below

Figure 1 – How our firm standards and High Level standards interact with our wider cryptoasset regime



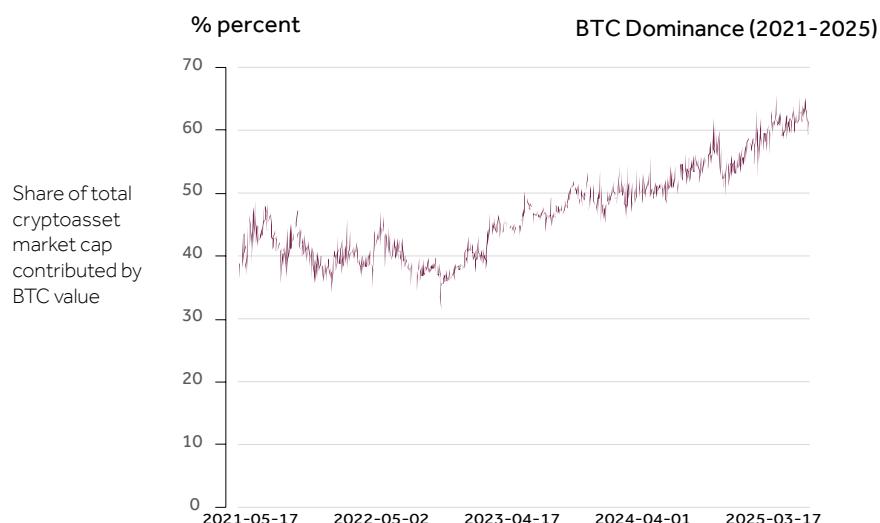
16. All firms authorised for regulated cryptoasset activities will need to comply with FCA rules for, firm standards such as Financial Crime, Senior Managers and Certification Regime, Operational Resilience, General Standards and Governance, Fitness & Proprietary, and High Level Standards (e.g. PRIN, COND, GEN). These rules are in addition to rules which currently apply to firms who are registered with the FCA under the MLRs, which will continue to apply.
17. For example, a firm issuing a regulated stablecoin from the UK would need to comply with our rules in relation to stablecoin issuance, including how they manage backing assets and their redemption policy. They would also face stablecoin-specific prudential requirements, based on their size and backing asset pool. In addition to these "stablecoin issuance" specific requirements, the firm will also need to comply with the wider FCA Handbook as set in this CP, including SYSC, PRIN, etc. These will be additional to rules which currently apply, including the MLRs and financial promotions.
18. Some rules we are proposing to apply to cryptoasset firms are subject to change, such as in CP25/21 (Senior Managers and Certification Regime). Impacts assessed within this CBA are based on current rules, and so the actual impact of our intervention in this CP may differ following any changes to the wider FCA Handbook. We will account for any subsequent changes in an updated CBA accompanying our Policy Statements.
19. This analysis presents estimates of the impact of applying FCA Handbook rules to cryptoasset firms. We provide monetary values for the impacts where we believe it is practicable to do so or otherwise provide a qualitative assessment. Our proposals are based on consideration of the expected impacts and judgement on the appropriate level of regulatory intervention.
20. HMT will publish an impact assessment (IA) alongside their SI which will estimate costs and benefits of bringing cryptoasset firms into the FCA's regulatory perimeter. Our CBA assesses the impact of the proposed application of FCA rules to firms being brought into the perimeter. We have assessed costs within this CBA on the basis that they are additional to what will be included in HMT's IA.
21. This CBA has the following structure:
 - The Market
 - Problem and rationale for intervention
 - Our proposed intervention
 - Options assessment
 - Baseline and key assumptions
 - Summary of impacts
 - Benefits
 - Costs
 - Competition assessment and wider economic impacts
 - Monitoring and Evaluation

The market

22. The term 'qualifying cryptoasset'¹ takes its meaning from the draft legislation published by the Treasury. These include assets such as Bitcoin, Ethereum, Stablecoins, and other community and utility tokens, in addition to so-called "memecoins" such as Dogecoin. While initially popular with privacy advocates as an alternative to currency, our consumer research indicates cryptoassets today are primarily considered as an investment product by UK consumers, (although, not exclusively so).

23. As of July 2025, the size of the global cryptoasset market was reported as \$3.3trn,² based on market capitalisation at current prices. A small number of popular assets make up the majority of the total market cap. In addition, a trend we have observed in recent years (post-2022) is Bitcoin increasing its share of total market value, from 41% in January 2023, to over 60% in July 2025.

Figure 2 – Increase in popularity of Bitcoin in recent years



24. Currently, the global cryptoasset market is characterised by limited regulatory oversight, with firms operating in the sector typically facing lower standards of regulation relative to equivalent products in existing financial markets. A recent trend we have also observed is listed companies announcing a strategic reserve of certain cryptoassets such as Bitcoin. There is evidence that establishing these reserves has had positive impact on company share price (MicroStrategy's, which maintains a Bitcoin reserve, saw its share price increase 400% throughout 2024, with reporting suggesting this was in part driven by increases in Bitcoin prices).

The UK cryptoasset market

25. According to our Cryptoasset Consumer Research Series (with Wave 5 published in November 2024), the most common reasons stated for owning cryptoassets are as "part of a wider investment portfolio" and "as a gamble that could make or lose

1 Cryptoassets are sometimes referred to as "cryptocurrencies", "digital assets" or simply "crypto".

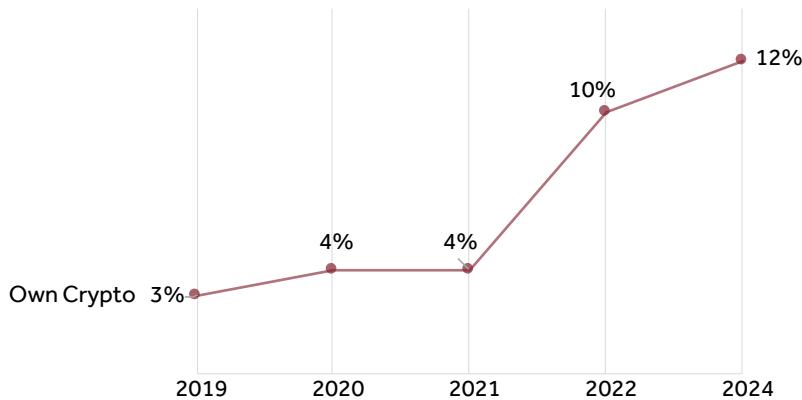
2 As reported by <https://coinmarketcap.com/>

money". Research conducted through the Digital Regulation Cooperation Forum (DRCF) highlighted financial returns as the primary motivator for UK consumers to buy cryptoassets, with consumers also valuing the "culture" associated with cryptoassets and the opportunity to make high returns in a short period of time.

26. UK demand for cryptoassets has increased sharply in recent years. FCA survey data indicates that ownership rates among UK adults have more than doubled since 2020, with our Consumer Research series estimating 7 million crypto owners across the UK as of August 2024 (12% of adult population).

Figure 3 – Consumer demand for crypto (Cryptoasset Consumer Research Series)

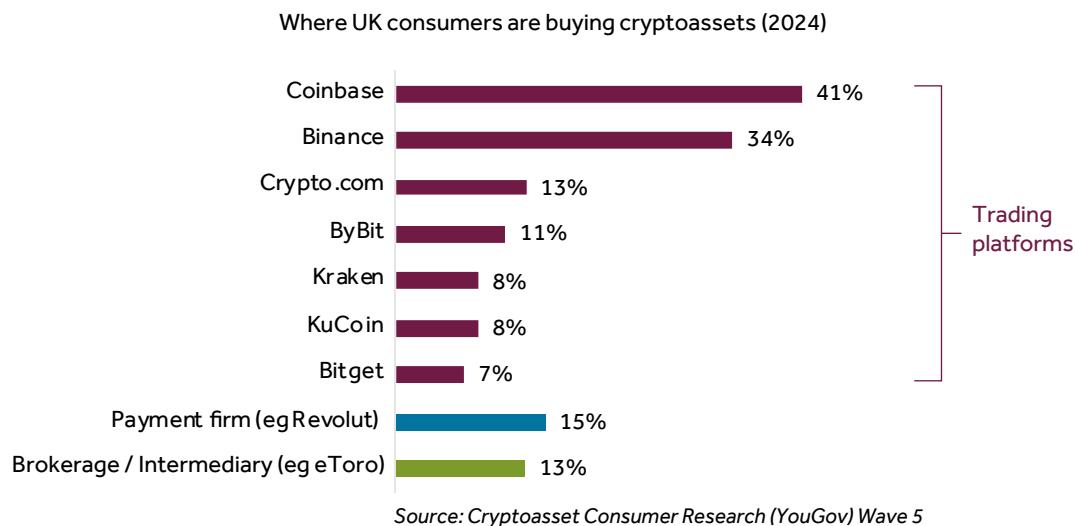
An estimated 7 million UK adults now own cryptoassets



27. Our Cryptoasset Consumer Research indicates that, as of August 2024, UK cryptoasset consumers hold a mean average of £1,850 worth of cryptoassets, with the median consumer holding around £500. Consumers with smaller portfolios are more likely to consider cryptoassets a speculative gamble, while those who hold larger volumes are more likely to view it as an important element of their investment portfolio. Cryptoasset consumers tend to be younger, male and earn above average incomes.

28. The majority of UK consumers rely on a small number of popular trading platforms and payment providers for purchasing cryptoassets as demonstrated below (note consumers may purchase from multiple sources and so figures below sum to greater than 100%). Our consumer research indicates cryptoasset holders have a high degree of trust towards these firms, driven by their longevity operating in cryptoasset markets and having large user numbers. The most popular trading platforms with UK consumers are domiciled in overseas jurisdictions, with our consumer research suggesting US cryptoasset firms as being the most popular with UK consumers.

Figure 4 – Where UK consumers purchase cryptoassets



29. In terms of wholesale markets and institutional investors, reports by blockchain analytics firm Chainalysis suggests the UK has the 3rd largest market globally for raw cryptoasset transaction volumes (behind U.S. and India)³.

Firm business models and regulatory requirements

30. The largest and most popular firms currently operating in the UK market typically provide vertically integrated services to retail consumers, generating revenue and profits from fees. Many firms offer cryptoasset trading services to consumers (typically through a mobile app), while also offering custody services for any purchased cryptoassets. Firms may offer ancillary services such as staking or lending products to their customers. Many firms also offer products and services to wholesale clients.

31. Beyond firms generating revenue from fees on consumers buying and selling cryptoassets, firms may operate additional business models within UK cryptoasset markets. Certain firms may charge fees for providing custody services to clients, while offering high levels of security and transparency relative to what could be obtained from a trading platform. As outlined in CP25/14, firms may also seek to issue qualifying stablecoins from an establishment in the UK and generate revenue from the backing assets and fees.

32. In terms of regulatory requirements, firms located overseas will be subject to the regulatory frameworks within those jurisdictions. IOSCO has published a set of 18 policy recommendations for the regulation of cryptoassets, and many member associations have implemented or are in the process of implementing these recommendations to firms they regulate.

33. For firms that are not based in the UK but have UK-based customers, there are additional regulatory requirements. Cryptoasset firms who carry out business within the UK must register with the FCA and comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

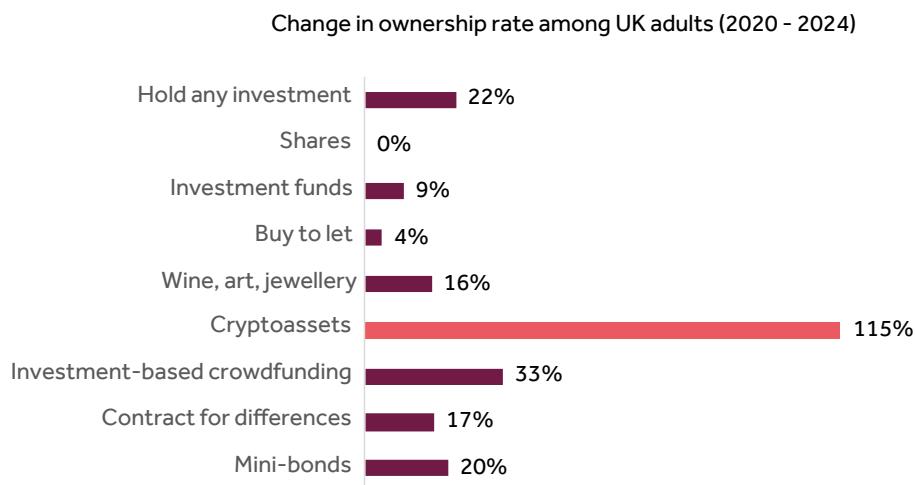
³ <https://www.cityam.com/uk-remains-worlds-third-largest-crypto-economy-and-biggest-in-europe/>

34. In addition to registering with the FCA and complying with AML/ CTF rules, firms also must comply with the Travel rule and collect transmit information about both the originator (sender) and beneficiary (recipient) of a cryptoasset transfer. Furthermore, since November 2023, cryptoasset firms offering products to UK consumers must also comply with our financial promotions regime.

Consumer outcomes and experiences

35. Evidence from our FLS indicates that since 2020, demand for cryptoassets among UK consumers has grown at a much faster rate than other assets we monitor, although from a lower base.

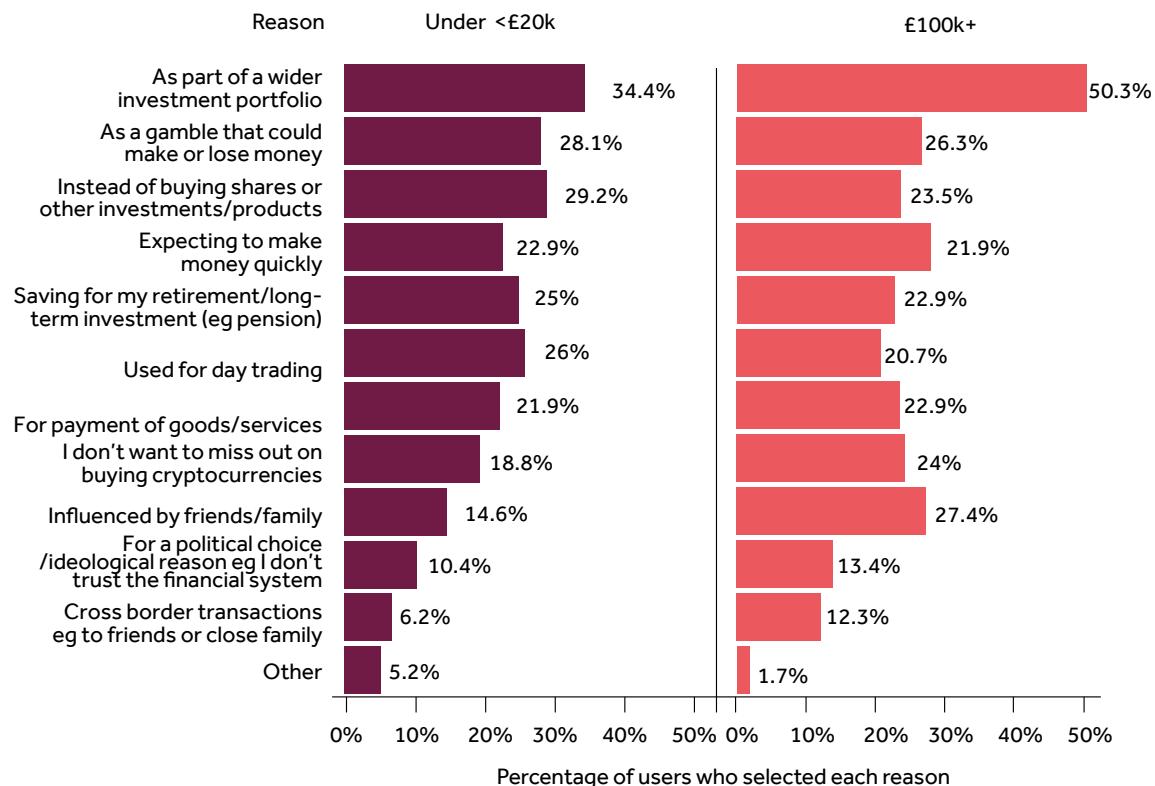
Figure 5 – How UK consumer demand for cryptoassets has changed relative to other investments



36. Our consumer research suggests that that growth in UK cryptoasset ownership is driven by several factors including increased accessibility (through user-friendly mobile apps), higher asset prices, and increased awareness in the media (particularly through celebrities and influencers).

37. While cryptoassets can have a diversity of functions, the most common reasons stated for owning crypto are as "part of a wider investment portfolio" and "as a gamble that could make or lose money", and this is our primary focus also. Research conducted through the Digital Regulation Cooperation Forum (DRCF) highlighted the financial returns as the primary motivator for UK consumers to buy crypto. A small share of consumers (~22%) currently purchase cryptoassets for payments of good/services, although this may increase following FCA regulation of Stablecoin issuance.

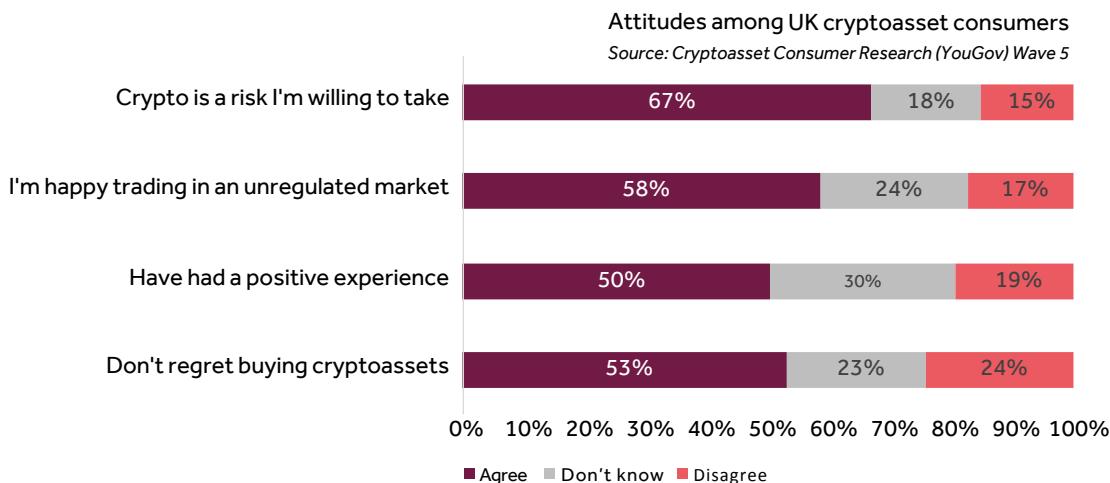
Figure 6 – Why people are purchasing cryptoassets (split by income)



38. Consumers tend to hold their cryptoassets on the platform they originally purchased them on, which is usually decided based on a recommendation of a friend or family member. Our consumer research suggests that this is supported by strong user satisfaction with Cryptoasset Trading Platforms. Our assessment of market dynamics is that consumers are reluctant to change platform once they have selected a platform, and so firms primarily compete in attracting new cryptoasset consumers. Firms largely offer homogenous products, so clients choose which firms they use based on trust, experience and advice from peers.

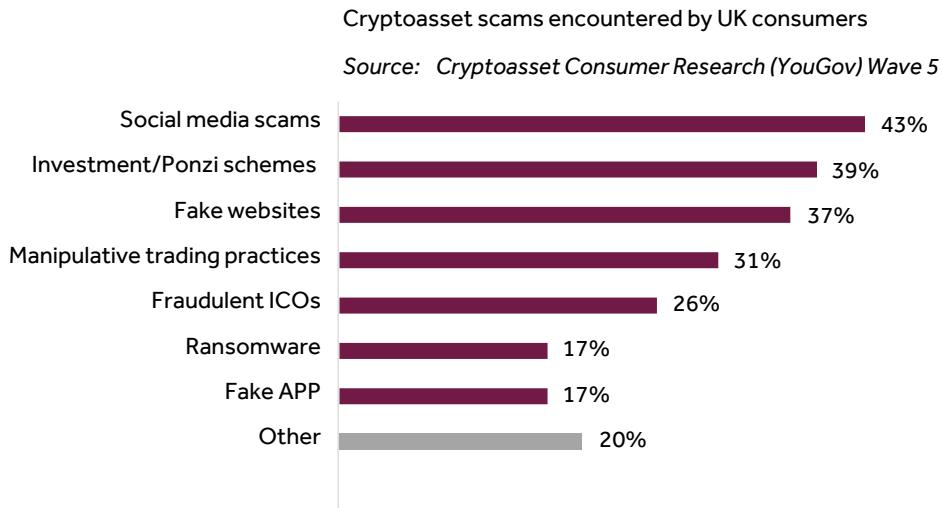
39. Consumers who own cryptoassets generally report positive experiences and are happy operating within the market even though they have limited regulatory protections. As illustrated below, most consumers are happy trading even though markets are unregulated, consider cryptoassets within their risk appetite, have had a positive experience, and generally do not regret their purchase. Many consumers also report that they would purchase more cryptoassets if they had a higher disposable income (63%) or if the market were regulated (49%).

Figure 7 – UK consumers experience of cryptoassets



40. However, despite positive sentiment reported by UK consumers, we have observed some consumers not receiving the right outcomes, with many consumers experiencing harm from frauds and scams. There were an estimated 9,000 cryptoasset scams or frauds reported to the FCA in both 2022 and 2023 in the UK, compared to approximately 3,000 in 2020. For comparison, our Financial Lives Survey (FLS) data suggests “Banking and Payments” related frauds and scams (such as APP) increased by about 30% during this time period (from affecting 10% of adults in 2020, to 13% in 2024).

Figure 8 – Frauds and Scams in UK Cryptoasset markets



41. Our consumer survey data suggests that many cryptoasset consumers have been subject to scams or fraud. 10% of UK cryptoasset consumers indicated that they lost money due to fraudulent activities involving cryptoassets, while an additional 17% indicate they were targeted for a scam but did not lose money. The most scams encountered were social media scams (43%) and Ponzi schemes offering unrealistic returns (39%).

42. Consumers who have experienced fraud represent a small portion of the total market, and the most common frequently reported amount lost was less than £500 (40%). 2% of consumers indicated they have lost more than £10,000 to fraudulent cryptoasset activity.

43. Other than fraud, many firms have relied on unsuitable business models or have taken excessive risks, as demonstrated in the market crash in 2022. Although still low, interconnectedness between cryptoasset and financial markets may be with stablecoins increasingly being suggested as a means of payment as well as settlement, and reports suggesting some US banks are considering offering loans backed by clients' cryptocurrency holdings.

Problem and rationale for intervention

44. Currently, a minority of UK consumers (around 1 in 8 adults) engage with cryptoasset markets, with those who do typically considering cryptoassets an investment which may potentially earn them high returns quickly. As outlined through our consumer research, most consumers are content with the market being unregulated and the limited protections in place (although most would also welcome additional regulation).

45. However, financial crime remains a key harm in relation to cryptoassets, which are appealing to harmful actors due to their lack of regulatory oversight and cross-border nature. There was an estimated \$40bn transferred globally to illicit address in 2024⁴, with the NCA estimating between \$1.7bn – \$5.1bn in illegal UK crypto transactions annually. In addition, fraudulent activity and scams occur regularly in cryptoasset markets, and when they do, consumers have limited remedies in the event they experience harm.

46. Many of the harms we observe in cryptoasset markets materialise due to how firms conduct themselves and engage with consumers. While we already regulate to reduce some harms such as money-laundering and terrorist-financing, other harms such as frauds and scams are not regulated in cryptoasset markets in the same way as other FSMA firms.

47. In the absence of specific regulation addressing them, these harms are likely to continue. While our activity specific rules will reduce some risks, wider harms associated with financial crime would likely remain. There is a risk introducing our activity specific rules will create a "halo effect" for consumers who believe they provide similar protections as comparative financial products.

Harms we are seeking to reduce in the UK cryptoasset market

48. We have observed harmful outcomes in cryptoasset markets which are driven by limited regulation and poor firm conduct, and which have adversely impacted UK consumers. These include:

- **Consumers buying unsuitable products:** Many UK consumers are unaware of the risks they are currently exposed to when engaging with cryptoasset markets. Lack of regulation and standards for how firms engage with consumers may result in consumers being misled on the assets they invest in or encouraged to buy products that are not suitable to them. This has included consumers being offered certain assets which are high risk or encouraged to engage in activities without being made fully aware of the risks. Recent examples include:
 - *Firms not being transparent on risks:* During the period 2020-2022 cryptoasset markets underwent a strong increase in demand for lending products. However, many firms providing these activities did not clearly communicate the risk associated with these products. This may have resulted in some consumers being unaware of the level of risk they were taking on when purchasing these cryptoasset and associated products, ultimately resulting in harm when several of these firms (Celsius, BlockFi) failed.
 - *Consumers permitted access to complex products:* Prior to their ban in 2021, many trading platforms allowed UK consumers to access cryptoasset derivatives, despite limited evidence to suggest consumers understand leverage or margin calls.
- **Cryptoassets being used for Financial Crime:** As noted, financial crime is a key harm associated with cryptoassets, which are appealing to criminals due to limited oversight and global nature. Examples of cryptoassets being used for financial crime include:
 - *Cryptoassets used for Fraud:* In May 2024 two individuals were convicted for stealing over £5.7m in cryptoassets, having fraudulently interpreted a cryptoasset trading platform.
 - *Cryptoassets use for money-laundering:* Also in May 2024, in a widely reported case, an individual was convicted for entering into a money laundering arrangement for £2bn and having attempted to use the proceeds to purchase properties.
- **Operational disruptions affecting market integrity:** Disruptions to the services that firms provide can potentially cause harm to both consumers and wider market integrity. They can prevent consumers from accessing their investment products in a timely fashion, which can result in stress, reduced choices and poor consumer service and treatment. Harm to other market participants can arise from, for example, the failure of a shared infrastructure on which the market depends, loss of access to market data to price trades, or the inability to complete post-sale activity. Operational risk management challenges are highly complex in cryptoasset markets, due to the nature of DLT and the risk of cyber attacks. Examples of recent operational disruptions in cryptoasset markets include:
 - *Consumers unable to withdraw funds:* In April 2025, a number of cryptoasset trading platforms temporarily halted withdrawals following a disruption at a 3rd party software provider.

- *Firms unable to complete trades:* Some of the more widely used DLT platforms for cryptoassets have suffered from repeated outages, halting transactions and reducing trust and confidence in the market.
- **Poor firm governance and conduct:** Conduct we observe in cryptoasset markets is often below what we would consider acceptable for authorised firms operating in UK financial markets and arises due to the absence of clear regulatory standards. Our analysis of markets suggests many firms fail to communicate clearly about their internal systems and controls, or in certain cases mislead consumers on important factors such as their cyber security arrangements. These aspects of firm governance represent a significant risk in cryptoasset markets due to the immutable nature of blockchain technology). Furthermore, a lack of conduct requirements for senior managers in cryptoasset firms may result in excessive risk taking or poor internal accountability. We have observed repeated instances of consumer harm as a result of unacceptable conduct by cryptoasset firms, including:
 - *Firms having inadequate internal controls:* Cryptopia, a New Zealand based Trading Platform lost approximately 10% of its cryptoassets in 2019 after they were stolen directly from a company wallet.
 - *Firms exposed to a Single Point of Failure:* Quadriga, a Canadian exchange relied on a private key to the firm's wallets holding clients' assets which was known only by the firm's CEO. The CEO's unexpected death in 2018 led to clients losing access to their assets with no possibility of recourse

49. These harms impact individuals who choose to engage in cryptoasset markets, and so their impact on the wider UK economy is currently limited. However, as cryptoassets have grown in popularity, the risk of harmful behaviour from firms spilling over and adversely impacting the wider UK financial services sector has increased. This is driven by several interrelated trends including:

- Increased cryptoasset ownership and amount of cryptoasset owned by UK consumers, which could mean a sudden downturn in cryptoasset prices could adversely impact a significant share of the UK public.
- Greater interconnectedness between the existing financial sector and cryptoasset firms, caused partly by higher retail demand and the fast-evolving market⁵. This may mean banks and other financial institutions could be negatively impacted by a downturn in cryptoasset markets.
- Use of strategic cryptoasset reserves by several publicly listed companies, which may increase their exposure to cryptoasset price shocks.

50. Due to these trends, UK consumers (including those who do not own cryptoassets) are more exposed to negative shocks in cryptoasset markets than previously. This creates risk of harmful side-effects to wider financial markets and the UK economy as a result of lack of regulation in cryptoasset markets.

⁵ <https://www.fsb.org/uploads/P170723-2.pdf>

How divergent nature of cryptoassets may exacerbate harms

51. The risk of harm may be greater for qualifying cryptoassets compared to traditional finance due to unique features associated with cryptoassets, including:

- **Geographical scope:** Most UK consumers (70%) rely on cryptoasset trading platforms based overseas. This creates a risk of harm in the event of insolvency – while it may be possible for an insolvency application to be made to a UK Court, it is more likely that an overseas firm will be subject to the insolvency regime and procedures of the firm's home state. This is further complicated by issues associated with evidencing ownership rights, vertical integration, the nascent nature of the market resulting in firms having a lack of familiarity with financial regulation.
- **Legal uncertainty:** There is greater legal uncertainty around ownership and location of cryptoassets compared to custody assets in traditional finance. There is no generally accepted legal definition of cryptoassets, or whether cryptoassets qualify as property (though the Law Commission concluded they likely do) and therefore are subject to ownership rights.
- **Digital nature of assets:** The pseudonymity of wallet addresses, append-only nature of many blockchains and consensus mechanisms for validations mean that, once cryptoassets are moved to particular wallets, it is almost impossible to access them without the wallet's private key. This can mean, unlike traditional financial assets such as stocks or property where possession can be reestablished, cryptoassets may be irrecoverable following a hack or the loss of a private key.

52. Some of these harms may be mitigated by existing FCA regulation, such as money laundering rules and financial promotion requirements. In addition, our planned regulation for cryptoassets will reduce legal uncertainty and require firms engaging with UK cryptoasset consumers to be FCA authorised, which may further reduce harm. However, we anticipate most of the harms above would continue to materialise in the absence of regulation addressing them, due to the drivers of harm, which are market failures, as discussed below.

Drivers of harms

53. We believe the above harms related to firm conduct and governance materialise due to negative incentives and feedback loops within cryptoasset markets. The drivers of harm are market failures which include information imbalances, optimism bias and other behavioural distortions:

- **Information asymmetry:** Cryptoasset firms and their employees have more information on their business models and practices than their customers. This can result in firms behaving in a way that is not optimal from the perspective of their customers because customers have incomplete knowledge about the firm's actions. Harm can materialise when customers act based on their limited information set that they would not have taken had they complete information, as they assume similar levels of firm standards and governance as when engaging

with other financial products⁶. For example, many consumers who relied on the trading platforms Celsius and FTX may not have done so had they been aware of internal governance structures and business model practices of these firms. Harms from information asymmetry can be further aggravated by behavioural biases, which can result in consumers taking excessive risk or conducting minimal research prior to purchase.

- **Behavioural distortions.** Cryptoasset prices have risen significantly in recent years, and this appreciation has resulted in many consumers expecting prices will continue to rise in the future. FCA research from May 2024, based on interviews with UK consumers, highlighted both a strong culture of optimism and a "fear of missing out" (FOMO) on popular assets within the sector. Consumers also demonstrate 'herding' behaviour, often relying on the activities of their peers or endorsement by celebrities/ influencers to support their decision making. Due to the behavioural biases, consumers may underestimate the likelihood of harm and engage in unintended or inappropriate levels of risk-taking.
- **Inadequate or misaligned incentives:** Firms may face weak incentives to adjust their behaviour and align their activity with the best interests of consumers. While consumers would benefit from a more transparent and risk-mitigating approach, firms can have limited reason to do so, as it would likely increase their costs. As noted, cryptoasset consumers exhibit evidence of herding behaviour by relying heavily on advice from peers and conduct limited research prior to investment. This has resulted in demand concentrated in key products and firms, creating weak competitive pressures and incentives for those firms to mitigate against harms.

54. Our intervention will only address these drivers of harm from UK-authorised cryptoasset firms. Global regulation will help to mitigate some of these harms, but UK markets will be primarily affected by UK-authorised firms. Cryptoasset firms who provide these services to UK retail consumers will be caught by the geographic scope of HMT's draft SI. The FCA, through its experience regulating cryptoasset for AML/CTF and financial promotions, is best placed to deliver a new regime for cryptoassets which can mitigate harms to consumers, while being proportionate to firms and encouraging future financial innovation.

Our proposed intervention

55. We are designing a regime based on our operational and strategic objectives, with a view to mitigate the risks cryptoasset firms may present. These are:

- Protecting Consumers
- Supporting Market Integrity
- Promoting Competition

⁶ Our 2024 qualitative research published through the DRCF highlighted that many consumers considered Cryptoasset firms as equivalent to other banking services they used, in part due to the nature of how they accessed products (via an application on their phone).

56. Our intervention will look to achieve these objectives through reducing risk factors which drive harm, while encouraging innovation in UK financial services markets. These risks include poor internal governance and control within firms. In addition, by providing regulatory clarity to firms, we are aiming to support market integrity and promote fair and effective competition.

57. Our intervention also furthers our Secondary International Competitiveness and Growth Objective through creating a well-functioning cryptoasset market. Our intervention is not seeking to encourage UK consumers to purchase cryptoassets and instead aims to ensure that those engaging with the sector can do so with appropriate regulatory protections in place.

58. Our proposed intervention is intended not to disproportionately burden firms and instead provide the appropriate levels of consumer protection we believe necessary to reduce harm. Our intervention looks to create a level playing field between cryptoasset firms and non-cryptoasset firms we regulate, by applying the same requirements for firms operating within UK requirements.

59. The outcomes we are seeking to achieve include:

- **Effective competition** that delivers high quality offerings and drives innovation in the UK cryptoasset sector.
- **Firms delivering good outcomes for retail customers**, including designing products and services that meet customers' needs and support when they need it. Firms must act in good faith, avoid foreseeable harm, and enable customers meet their financial objectives.
- **Cryptoassets used within our regime are not attractive for financial crime**, including fraud, money laundering, terrorist and proliferation financing or any other criminal activities.
- **International competitiveness of the UK economy is supported**, as well as its growth in the medium to long term, and firms are encouraged to set up in the UK to offer cryptoasset products and services.
- **Well-run firms with appropriate standards and resources**, which means they are well placed to put matters right when things go wrong, with clear, proportionate standards which can be supervised effectively.

60. In identifying how intervention in this market can support both FCA strategic and operational objectives, we consider our approach from a perspective of "**rebalancing risk**". This approach recognises the important role risk-taking plays in driving innovation and delivering benefits for consumers in financial services markets, whilst also reducing harm where needed. In "rebalancing risk" we look to assess the relationship between the benefits being sought and the potential harm that could be caused in pursuing these benefits. This approach is not about accepting harm, but rather about ensuring we make balanced, risk-informed decisions that reflect the real-world complexity of dynamic markets, and allow us to be a smarter, more adaptive regulator.

61. To assess our policy intervention within the context of rebalancing risk, we consider the following:

- There are trade-offs when making choices for policy interventions, and that the FCA does not operate a zero-fail regulatory regime.
- There may be a risk 'safety zone' where an increase in risk can deliver benefits without significant impacts on harm.
- As the level of risk increases, there may be a 'danger zone' where harm starts to outweigh the benefits from increased risk taking and we would want to avoid this space.
- Consistent with the approach set out in our Statement of Policy on CBAs, we also account for distributional impacts, particularly in determining who bears risk and how well equipped they are to bear the risk

62. Applying this approach within the context of cryptoasset markets, while we expect our proposed intervention to significantly reduce the harms, we anticipate some harms will continue to occur. For example, our proposed intervention will not seek to regulate DLT-platforms or require that these platforms become FCA authorised. This could result in continued harm to consumers, if for example a widely used DLT-platform experiences frequent outages which damages consumer trust and market integrity. We do not believe this illustrative harm, or similar harms that may continue post-regulation will be widespread or create systemic risk, and that accepting some harms will continue is necessary to ensuring our regulation is proportionate to firms and providing opportunities for growth which benefit consumers. This has informed our overall policy interventions and consideration of a range of options.

63. In order to achieve these outcomes, our proposed intervention will apply existing FCA cross-cutting sourcebooks to firms carrying out regulated cryptoasset activities. These sourcebooks already apply to Part 4A authorised firms and we propose they will apply to cryptoasset firms as Part 4A FSMA authorised firms under our future cryptoasset regime.

64. Specific requirements we propose applying to cryptoasset firms include:

- **High Level Standards:** We propose that firms will have to comply with our 11 principles for Businesses. This includes conducting business with integrity, maintaining adequate financial resources and managing conflicts of interest fairly, both between itself and its customers and between a customer and another client.
- **Firm Standards and Governance rules:** We propose that firms authorised for regulated cryptoasset activities should be required to comply with our Senior Management Arrangements, Systems and Controls (SYSC) sourcebook. This requires firms to organise and control their affairs responsibly and effectively, with adequate risk management systems. This includes:
 - **Senior Managers and Certification Regime:** We propose to apply all the existing elements of SM&CR to cryptoasset firms, in line with the current approach for existing financial services. This approach also involves applying all relevant senior management functions, certification functions, prescribed responsibilities and conduct rules.

We are aware the FCA's SM&CR Review Consultation and the Treasury's consultation to amend legislation for SM&CR are both currently seeking

responses on their proposals. Given these proposals are still out for consultation, we are unable to apply these changes to cryptoasset firms at this stage and have applied the full cost of the existing SMCR. Firms should read this CBA alongside the CBA corresponding to our SMCR Review consultation paper.

- **Financial Crime:** We are proposing to subject cryptoasset firms to the same regulatory standards as all other Part 4A FSMA authorised firms. This involves the application of the Financial Crime provisions in SYSC 6, alongside the MLRs. Firms will need to become familiar with the FCA Financial Crime Guide (FCG) (which has been recently updated to include guidance for cryptoassets).
- **Operational Resilience:** Firms will be brought into alignment with existing operational resilience requirements under SYSC 15A. Firms must identify important business services which could cause harm if disrupted. For each business service, they must set an impact tolerance and have a comprehensive understanding of how to deliver each important business service.
- **Sustainability rules:** Anti-greenwashing rules as set in the ESG sourcebook will apply to cryptoasset firms

Addressing market failures through our proposed intervention

65. Applying these Handbook rules to cryptoasset firms will help address the market failures we have outlined and ultimately lead to better governance and accountability within the firms that we regulate. These market failures, which drive the harms we observe in the market can be substantially mitigated through our proposed intervention, which will improve firm governance, transparency and accountability.

66. How we anticipate our specific intervention to address the identified market failures is outlined in the table below.

Market Failure	Addressed by Intervention
Information Asymmetry	<ul style="list-style-type: none">• High Level standards, which will require firms to pay due regard to the information needs of its clients.• SM&CR rules, by encouraging better decision making within firms and improving regulatory oversight.• Operational resilience requirements, through making firms more aware of their limited information and vulnerabilities and being able to better account for them and prevent disruptions.
Behavioural Distortions	<ul style="list-style-type: none">• High Level standards, which will require firms take reasonable care to ensure the suitability of its advice and discretionary decisions for customers who are entitled to rely upon its judgment.• SM&CR rules, through increasing accountability within firms, improving trust among consumers and reducing harm arising from behavioural biases.

Market Failure	Addressed by Intervention
<i>Misaligned Incentives</i>	<ul style="list-style-type: none">• High-Level Standards, which will require firms to manage conflicts of interest fairly, both between itself and its customers• SM&CR rules, through increasing senior manager accountability, driving up culture and standards in cryptoasset firms and allowing firms to better detect and address misconduct. This helps counter weak incentives firms may currently face to address these risks.• Operational Resilience requirements, by placing a high-level of accountability on firms to identify risks of disruption and planning for them accordingly. This helps counter weak incentives firms may currently face to address these risks.

67. As outlined above, we expect our proposed intervention will help address the market failure identified primarily through increasing accountability of firms and senior managers. In mitigating the presence of these market failures in UK cryptoasset markets, we expect the harms we currently observe in these markets to be significantly reduced, as we have observed traditional financial markets we regulate.

68. Some of the harms identified also arise or are aggravated by volatility within cryptoasset prices, which operates which operates continuously (i.e. 24/7) within a highly interconnected global market. For example, consumers may purchase unsuitable products which do not fit their risk appetite due to behavioural heuristics (e.g. optimism bias, herding behaviour), which can result in harm if asset prices change suddenly. Our regulation will not prevent volatility within cryptoasset prices and instead look to ensure that consumers are well-informed of risks, and firms act with high levels of conduct and accountability.

Options assessment

69. Our proposed intervention will apply existing FCA Handbook rules to firms conducting regulated cryptoasset activities, following the principle of "same risk, same regulatory outcome". This design principle is technology agnostic while also considering whether the technology, or its use create additional risks.

70. In identifying our proposed intervention, we considered alternative options which sought to achieve similar outcomes. Options were assessed in terms of how well they would support FCA Strategy and Objectives, constraints and delivery risks, in addition to any unintended consequences they could create. We set these out below, in addition to their relative limitations that led us to dismiss them.

Alternative option: Apply sustainability disclosures to cryptoasset firms

71. Cryptoasset firms will be required to comply with anti-greenwashing and marketing rules as a result of being FSMA-authorised firms. However, we could go beyond this and introduce sustainability disclosure requirements for firms. Introducing sustainability

requirements for cryptoasset firms could increase awareness of the different environmental impacts of particular tokens and allow for more informed decision-making that aligns with consumer investment preferences. This would also mirror the approach taken by the EU's cryptoasset regime (MiCA), which requires reporting on an asset-level basis

72. However, we consider there is not enough data to ensure consistent standards for cryptoasset specific sustainability disclosures. In addition, consumer research from Mintel⁷ suggests only a small number of UK cryptoasset consumers have concerns about the environmental impact, indicating it is unlikely their behaviour would be changed by sustainability disclosures.

Alternative option: Create specific Senior Manager roles for Cryptoasset firms

73. Within our discussion paper DP23/4 (stablecoins), we outlined the possibility for tailored requirements for authorised cryptoasset firms (e.g. new enhanced criteria, more focuses certification functions and additional SMFs). This approach could potentially better account for cryptoasset specific business models and reduce risk to firms and consumers.

74. However, in the feedback to our DP, we did not receive strong indication from firms that specific roles were needed, and instead it was suggested that the existing Senior Manager framework would work within a cryptoasset context. Furthermore, specific tailoring for cryptoasset firms would likely result in greater costs to firms to adhere to tailored rules, upskill staff and engage with the FCA.

75. A summary of our options analysis is presented below:

	How it would support FCA Strategy and Objectives	Constraints and delivery risks	Likelihood of unintended consequences	Overall Assessment
Apply sustainability disclosure requirements to Cryptoasset firms	Increased awareness for consumers and alignment with EU regulatory approach	Poor data quality may result in lack of consistency or comparability	Low, although poor data quality could result in unexpected outcomes	Limited evidence to suggest it would impact consumer behaviour
Create specific Senior Manager Functions	Higher costs to firms, but may be better able to account for cryptoasset specific business models	Limited evidence to suggest specific roles are needed	Inconsistent with wider SM&CR approach	Unlikely to be more effective at delivering on our objectives relative to proposed option.

	How it would support FCA Strategy and Objectives	Constraints and delivery risks	Likelihood of unintended consequences	Overall Assessment
Same Risk, Same Regulatory Outcome (Proposed option)	Consistent with global approach. Risks to consumers are reduced but not eliminated	Consistent with current FCA approach to FSMA-authorised firms.	Risk of halo effect of regulation	Reduces harm while also creating opportunities for innovation.

76. We believe our proposed approach is the most effective option for meeting our statutory objectives and reducing harm in the market. Our proposed option supports a level playing field across authorised cryptoasset firms, and other FSMA-authorised firms we regulate. Both sets of firms will face similar regulatory standards and we anticipate this technology-agnostic outcomes-based approach will create a framework for increased technological innovation through use of DLT.

Causal chain

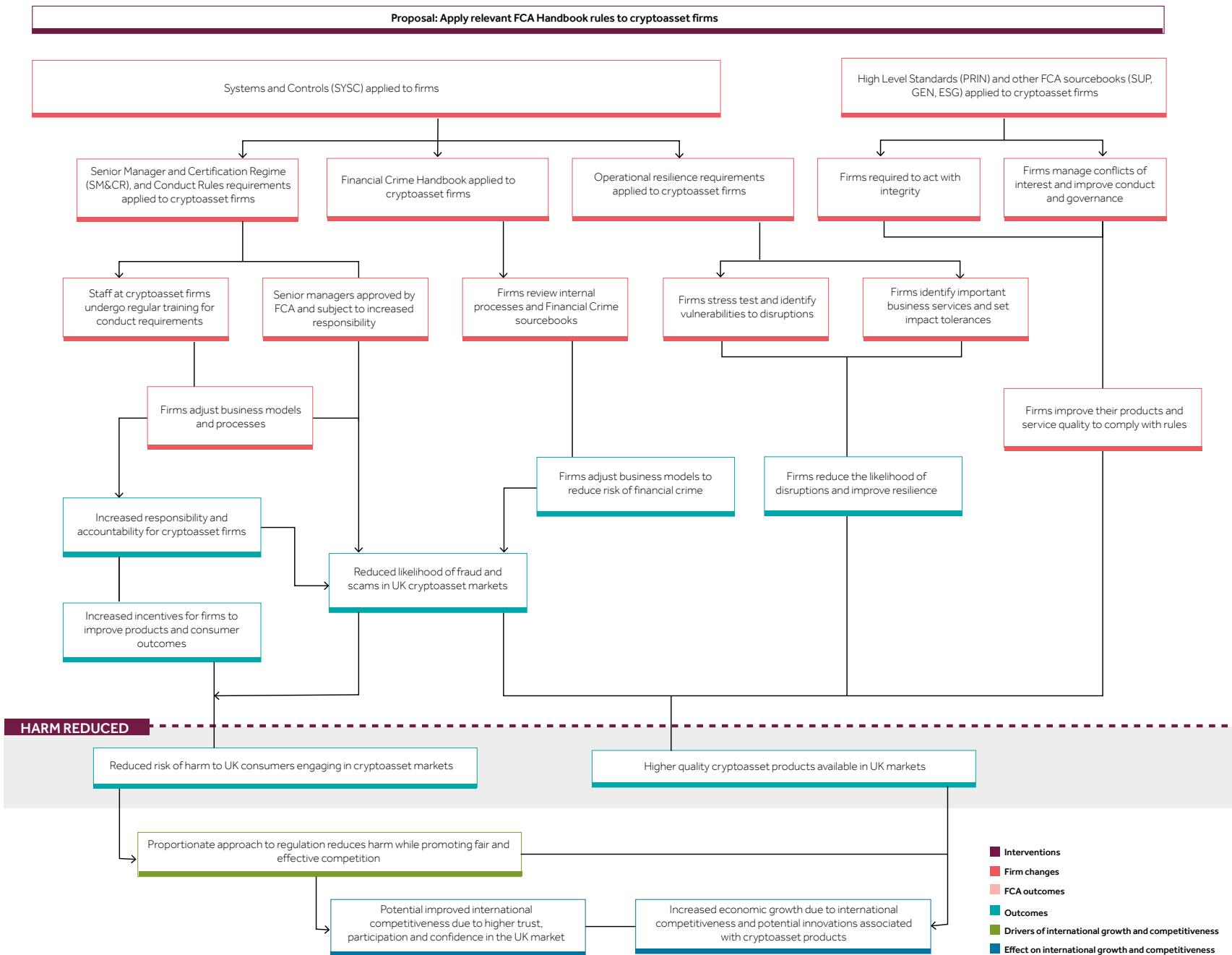
77. The below figure presents the causal way we expect the above changes will improve outcomes for consumers and support our secondary competitiveness and growth objective. Our interventions seek to reduce harm to consumers and the wider markets, rather than operate a zero-failure regime.

78. Our causal chain demonstrates how we expect our regulatory intervention results in changes in the market which have knock-on effects which ultimately result in reduce harm for consumers. Nodes within the chain have been informed by relevant academic literature⁸ and our understanding of consumers that we have established through our surveys and firm engagement.

79. Our key assumptions are:

- Firms change their behaviour as a result of our intervention, including adjusting business models in line with our proposed requirements.
- Introducing regulation provides greater clarity and regulatory certainty to firms, which results in increased market entry.
- Consumers respond to increased regulation by increasing demand for cryptoasset products. Higher demand, combined with regulatory clarity to firms, results in market entry, which promotes competition in the market.
- Firm standards and governance rules, create strong incentives for firms to minimise fraud and scams on their platforms.

⁸ Including "Makarov & Schoar, 'Blockchain Analysis of the Bitcoin Market, NBER, 2022" which provides detailed assessment and information about the behaviour of the main market participants, and "Gornelli, "Crypto shocks and retail losses", BIS, 2023", which outlines how consumers react to negative market events.



Our analytical approach

80. We assess the impacts of our proposed new rules against a baseline, or 'counterfactual' scenario, which describes what we expect will happen in the cryptoasset market (both domestic and international) in the absence of our proposed policy change. We compare a 'future' under the new policy, with an alternative 'future' without the new policy.

81. We constructed this baseline by looking at evidence of the current situation in the sector and extending this into the future. Our counterfactual is based on evidence from the following sources, which we discuss in more detail in the following subsection:

- Surveys and engagement with cryptoasset firms.
- Consumer data
- Previously published FCA Cost Benefit Analyses
- Our experience and knowledge of the costs associated with regulation, including using our Standardised Cost Model (see Annex 1 here).

82. We consider the impact of our proposals over a 10-year period with costs and benefits occurring from the assumed time of implementation. We account for any costs and benefits arising from moving between the interim and end-state rules. When estimating net present value of costs and benefits, we use a 3.5% discount rate as per Treasury's Green Book. Prices are provided in 2025 figures.

83. We consider the assumptions below as comprising our "central scenario" as they represent our best estimate of the likely costs and benefits we expect to materialise from our proposals.

84. We recognise the currently unregulated nature of cryptoassets creates limitations for the accuracy of this central scenario, and our estimates and analysis above are subject to significant uncertainty. To account for this uncertainty, we consider an additional scenario where the impact of our intervention is less effective than within our central scenario. We examine the impact of this additional scenario relative to the baseline in our sensitivity analysis below.

Surveys and engagement with firms

85. In February 2023 we sent cost surveys to firms we identified as potentially being in scope of our future cryptoasset regime. In total, we received 10 responses from firms, who provided both activity specific costs, in addition to cost estimates associated with complying with wider FCA rules (SM&CR, Operation Resilience, etc). We use these survey responses to develop cost estimates of our requirements on firms (uprating to 2025 prices).

86. In addition to cost surveys, in DP23/4 we outlined how we anticipated applying existing FCA Handbook rules to cryptoasset firms and included a short assessment on the types of costs and benefits we anticipated to materialise following our regulatory intervention. DP responses largely agreed with our assessment of the type of costs which would materialise, including both direct compliance costs and business model changes.

Consumer data

87. Since 2019, the FCA has published a regular series of cryptoasset research notes based on survey data of UK cryptoasset consumers. Our most recent publication (Wave 5, with fieldwork taking place in August 2024) involved over 3,000 respondents and provides us with the opportunity to identify trends in consumer behaviour. We use this survey data for estimating the current baseline in the market, and how demand for products could change following regulation.

88. In May 2024, in conjunction with the Information Commissioner's Office (ICO) through the DRCF we published a research note on consumer attitudes towards cryptoassets. This qualitative research further strengthens our understanding of the baseline, the behavioural biases of consumers and the likely demand-side response to our proposed intervention.

Previously published FCA CBAs

89. While our cost surveys to firms provide a strong baseline for assessing how firms will be impacted by our proposed intervention, the limited response rate creates a high degree of uncertainty. As a result, we have looked to supplement our estimates of likely costs through reliance on previously published FCA CBAs.

90. Several of the Handbook rule requirements we are proposing applying to cryptoasset firms have been consulted on in recent years. These consultations have been supported by CBAs, which have provided indication of the type of costs and benefits we could expect to materialise for firms subject to these areas of the FCA Handbook. In using cost estimates from previously published CBAs, we update cost estimates to our current price year (2025).

91. Reliance on these previous CBA estimates may result in additional uncertainty for our cost estimates, as it requires us to assume cryptoasset firms will incur costs at a similar rate as existing FSMA-authorised firms. We welcome feedback on potential limitations with this approach.

Data limitations

92. Our surveys and firm engagement have helped us in better understanding of how the cryptoasset sector currently operates within the UK, and the potential costs and challenges which may arise because of our proposed intervention. This is particularly true in our understanding of retail demand for cryptoasset, where our various research outputs have provided us strong insight into how and why UK consumers engage with cryptoassets. However, in gathering our data to assess the impact on firms, we faced several limitations which affect our analysis, namely:

- **Cryptoasset sector is new and fast-evolving:** Many firms who will be in scope of Treasury legislation and thereby affected by our rules are currently outside our regulatory perimeter and may have limited experience of the regulation our

proposed intervention would introduce. This makes estimating impacts uncertain, particularly where our regulation will result in significant changes to business models.

- **Limited responses to our cost surveys:** While we received responses to our cost surveys from firms, the volume of responses was lower than we typically receive from surveys of this kind,. While the cost estimates provided are used in our analysis, the smaller response rate makes aggregating responses for the "average" firm or identifying outliers more challenging.
- **Reliance on previous FCA CBAs and SCM:** To account for the limited survey response rate, we have used data from previously published FCA CBAs, and our Standardised Cost Model to assess likely impacts of our proposed rules to firms. However, these estimates and the SCM have been produced with reference to traditional finance firms regulated by the FCA. This creates a risk of underestimating or overestimating costs to cryptoasset firms, due to different business models they operate relative to traditional finance firms.

93. We have taken several steps to address any adverse impact of these limitations. To better understand costs to firms, we undertook a comprehensive review of cryptoasset related cost-benefit analyses (or equivalent) published by international regulators and used these to inform our evidence base. We have also used data from other areas we regulate cryptoasset firms, such as financial promotions, as assessed in CP 22/2 (financial promotion rules for cryptoassets). We have also conducted uncertainty and breakeven analysis below to better account for potential evidence gaps within our firm data.

94. While we recognise the limitations of our evidence base, we are satisfied it is of sufficient quality to estimate impacts of our proposed intervention.

Baseline for current UK cryptoasset market

95. Our starting point for our baseline is the state of the current market. Our most recent consumer survey research indicates:

- Cryptoassets are owned by 12% of UK adults, holding an average portfolio of £1,850.
- Centralised exchanges remain the most popular way for UK consumers to purchase cryptoassets, with 69% choosing to do so this way. The next most popular purchase journeys are through a payment firm (15%) or a brokerage (13%).
- 26% of cryptoasset consumers have been targeted by a crypto-related fraud or scam, with 10% losing money as a result.
- 32% of consumers have had some negative experiences when accessing their cryptoassets
- 20% of cryptoasset consumers believe they have financial protection when purchasing cryptoassets.

96. We assume that absent our proposed intervention, the harm we outlined earlier in this document will continue harming clients to the same degree over the next 10 years. The harm our intervention aims to minimise is in relation to firm conduct and governance for firms operating within the FCA's cryptoasset regulatory regime. Our intervention will also impact non-UK consumers if served by a firm established in the UK.
97. Our consumer research indicates that demand for cryptoassets within the UK is concentrated as a speculative asset which provides potentially high returns in short time periods. Consumers rely significantly on advice from friends and family and demonstrate optimism bias and herding behaviours.

Baseline for FCA regulation

98. Our proposed intervention will introduce the same regulatory requirements as currently apply to firms within our perimeter, to cryptoasset firms which will enter our perimeter. In developing our baseline for analysis, we consider how these Handbook rules currently apply to FSMA-authorised firms, and how this will impact cryptoasset firms over the course of our appraisal period.
99. However, many of the rules we are proposing to introduce to cryptoasset firms are themselves subject to potential future changes and amendments to how they are applied. At the time of publication of this CP, we are separately consulting on changes to our Senior Managers Certification requirements, and it is possible other rules we are introducing to cryptoasset firms will be changed over the course of our appraisal period. This creates additional complexity for establishing our baseline, as it requires us to make assumptions on how FCA regulation could change in the coming years.
100. For the purposes of our CBA, **we assume all Handbook rules as they currently apply to FSMA-authorised firms (as of September 2025) will continue to apply to firms in the same manner over the course of our appraisal period**. This includes areas where we are currently consulting on proposed changes to our rules. While this approach limits our analysis, we believe it is the most appropriate method to address the uncertainty. We will continue to monitor developments in the FCA regulatory perimeter, and account for any changes in an updated CBA accompanying our Policy Statements next year.

Key assumptions

101. In order to estimate the impact of our proposed rules, we require assumptions for our analysis. These assumptions are based on our understanding of UK and global cryptoasset markets, but are subject to significant uncertainty, particularly due to the novel and fast-evolving nature of cryptoassets. Our analysis is highly sensitive to these assumptions, and we welcome feedback and challenges on our assumptions.
102. We assume full compliance with new rules by cryptoasset firms. In addition, we assume greater regulatory clarity results in increased entry by firms into UK cryptoasset markets

103. We assume costs estimated for FSMA-authorised firms to comply with FCA regulation in previous FCA CBAs are reasonable approximations for costs cryptoasset firms will incur to comply with similar regulatory requirements.

104. Many firms that will seek authorisation under the FCA's cryptoasset regime may already be regulated by the FCA for other activities, and so already be familiar with our Handbook requirements. For simplicity, we assume all costs to firms are additional. Actual costs incurred by firms may be lower if they are already regulated and compliant with our rules.

105. In estimating volumes of fraud, we use data relating to "Investment Products" to approximate future frequencies in UK regulated cryptoasset markets. We assume these are the most appropriate comparison for the types of products and services cryptoasset firms will offer and so have provide an indication of the frequency of scams and frauds we might anticipate still occurring in cryptoasset markets following our intervention.

Assumptions on number of firms affected

106. Overall, we anticipate that firms of different sizes will incur different costs. We categorise firms as Large, Medium or Small based on our Standardised Costs Model (SCM). Firm populations are based on survey responses (both consumers and firms), in addition to our review of cryptoasset firms currently registered with the FCA and which may seek authorisation in the future⁹. As all firms taking part in a regulated FCA activity will be subject to our proposed requirements, our firm population represents our estimate of how many firms will be regulated within the FCA's cryptoasset regime, and is subject to significant uncertainty.

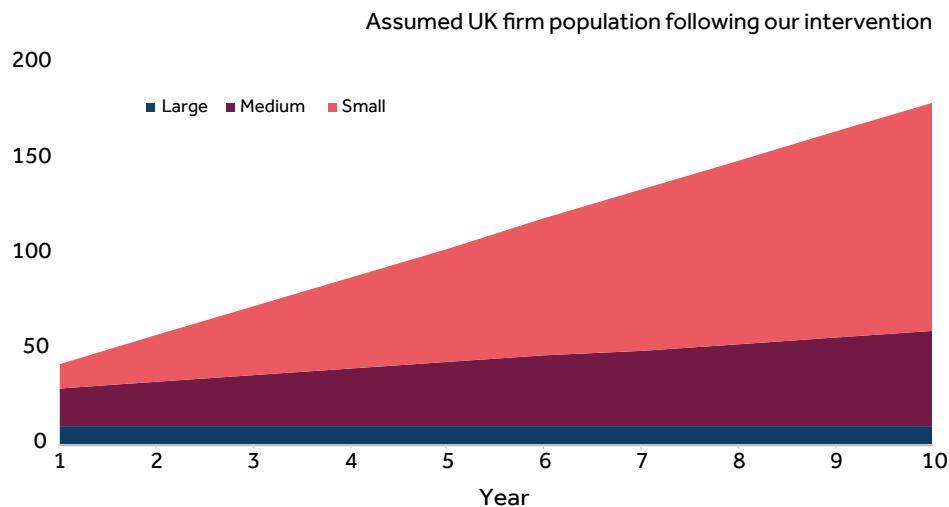
Estimated firm population

	Small	Medium	Large	Total
Cryptoasset firms	120	50	10	180

107. We assume larger firms will enter the market immediately, to avoid disruption to their current business operations. We assume most other firms will enter the regulated UK cryptoasset market gradually as they become familiar with our rules and requirements.

⁹ <https://register.fca.org.uk/s/search?predefined=CA>

Figure 9: Assume firm population

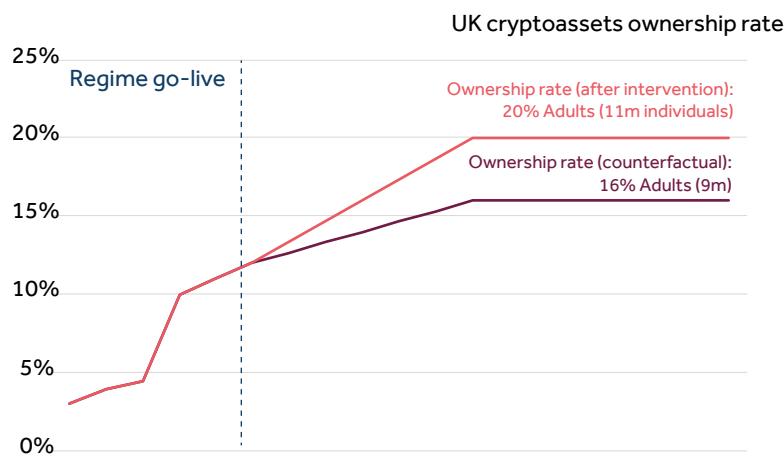


Assumptions on consumers

108. The baseline for our proposed change is that cryptoassets will remain popular with UK consumers, but demand would likely plateau in the coming years, as more risk averse individuals will not enter the market without some level of regulatory protections. We assume, without regulatory protections in place, the UK cryptoasset ownership rate will continue to increase (following trends in recent years) but will eventually level off slightly above the current ownership rate (and similar to levels observed currently in the US).

109. Following our intervention, we assume demand for cryptoasset increases. As outlined in our consumer research, a significant share (8%) of non-crypto owners indicate they would be more likely to purchase cryptoasset, even if this did not involve financial protections against losses¹⁰. We assume these individuals enter the UK cryptoasset market after our cryptoasset regulatory regime has been established. Estimated demand is outlined below:

Figure 10: Estimated demand



¹⁰ A much higher share of non-cryptoasset owners (26%) indicate they would be more likely to purchase cryptoassets if it included some form of financial protections against losses

110. The type of users may also change due to our intervention, with women and younger consumers more likely to invest in cryptoassets if regulatory protections are introduced. We assume any new users in the market hold similar portfolios as existing users, in both our proposed option and counterfactual.

Assumptions on the wider cryptoasset market

111. Our survey data indicates most cryptoasset firms used by UK consumers are based internationally. Given uncertainty as to when international regimes will introduce regulation, and if they do so, whether that will introduce any protections for UK consumers of those overseas products or services, we assume any standards introduced internationally will not apply similar levels of protection for UK consumers as our proposed intervention.

112. We also make the following assumptions:

- Benefits result from imposing new requirements to firms within the FCA's regulatory perimeter and not what other jurisdictions impose elsewhere.
- The overall regulatory treatment of issuers of cryptoasset firms aligns with other IOSCO jurisdictions (e.g. EU, Singapore) in the long-term. Therefore, the risks related to regulatory arbitrage are low.

113. And use the following terms:

- Unless stated otherwise, all references to 'average' are the mean average.
- All price estimates are nominal.

114. We note that the per-firm estimates we set out in this CBA have been generated to increase the robustness of industry-level estimates. Per-firm cost estimates correspond to the mean cost, and do not capture the potentially wide range of costs that a particular firm may incur. For the avoidance of doubt, individual firms may in practice bear costs greater or lower than the per-firm averages used to estimate overall costs to the industry. This will depend, among other things, on the firm's individual size, makeup, and current practices. Firms should consider our proposals in relation to their specific operation and provide feedback on this basis, supported by evidence where they believe costs differ.

Accounting for differences between cryptoasset firms/products and other FSMA-authorised firms/products

115. While cryptoassets share many similarities to other High-Risk Investment products and services we regulate, there are important differences which may impact the effectiveness of our rules. These include:

- **Global nature of the market:** Cryptoasset markets operate a continuous, highly interconnected market which is cross-borders, with firms serving multiple jurisdictions

- **Multiple use for products:** In addition to being used as an investment product, cryptoassets may also be used for payment services, or as a governance token within a decentralised exchange.
- **Reliance on permissionless infrastructure:** Cryptoassets rely on DLT for verification of transactions, with the most popular being permissionless and decentralized in governance

116. In accounting for these differences within our analysis, we have looked to make use of our evidence base for the UK cryptoasset markets. For example, while cryptoasset products are used by some consumers for payments, the majority of consumers treat them as an investment product, and cryptoassets currently limited acceptance rate across UK retail merchants. As such, we have focused our analysis on their use as an investment product, which considering potential use cases elsewhere.

117. In addition, our proposed regulatory framework also looks to account for these differences, such as requiring firms to be authorised if they have any UK consumers, rather than only if they are located in the UK.

Summary of impacts

118. This section summarises benefits and costs associated our intervention, the net present value (NPV) over the appraisal period and the net direct cost to firms. The benefits and costs include those incurred by firms, consumers, the FCA and wider society. Some costs and benefits are direct, others are indirect. Direct impacts are unavoidable whilst indirect impacts depend on how consumers and firms respond. Costs and benefits will be both one-off, and ongoing.

119. The key expected benefits are:

- Improved market confidence/integrity/ firm efficiency due to regulatory clarity and consistency of standards and compliance.
- Reduced risks of harm to consumers, due to higher regulatory protections, and reduced likelihood of cryptoasset fraud and scams.
- Firms benefiting from increased demand for cryptoasset products due to higher regulatory standards leading to increased consumer entry.
- Increased competition in UK cryptoasset markets due to improved regulatory certainty, which benefits consumers through lower prices and higher quality products and services.

120. The key expected costs are:

- Compliance costs to firms, including IT and personnel costs, which will be both one-off implementation and ongoing costs for firms to comply with the new requirements
- Changes to business models as a result of our regulations
- Authorisation and supervisory costs for the FCA to ensure new and existing firms meet the requirements

- Halo effect from regulation, potentially resulting in increased consumer investment into cryptoassets, and substitution away from existing regulated financial products. This transfer may be a cost to the wider UK if it reduces retail demand for domestic investments.

121. A summary of our expected costs and benefits is set out in the table below:

Total Impacts (10-year PV)

Group Affected	Item Description	PV Benefits	PV Costs
Firms	Firm Standards (SYSC)		
	<i>Senior Managers and Certification Regime</i>		£9.8m
	<i>Financial Crime rules</i>		£2.6m
	<i>Operational Resilience</i>		£39.1m
	Other Requirements		
	<i>High Level Standards</i>		£1.1m
	<i>Additional Custodian requirements</i>		£40.1m
Consumers	Reduced Losses from scams	£130m	
Total impacts		£130m	£92.6m
Net Impact			+£37m NPV

122. The Estimated Annual Net Direct Cost to Business (EANDCB) from our proposals, affecting cryptoasset firms is set out in the table below.

	Total (Present Value) Net Direct Cost to Business (10 yrs) EANDCB	Total (Present Value) Net Direct Cost to Business (10 yrs) EANDCB
Total net direct cost to business (costs to businesses – benefits to businesses)	£92.6m	£9.5m

Benefits

Benefits to consumers

123. The primary benefits to consumers relate to reduced harm through greater regulatory protections, which we believe will save consumers from losing money relative to our counterfactual. We focus on the following benefits to consumers:

- **Reduced financial crime (including frauds and scams):** We expect our regulation to reduce the incidence of scams associated with cryptoassets, due to higher standards for firms.
- **Increased trust and regulatory certainty:** Our regulation will set clear standards and accountability for cryptoasset firms operating in UK markets. We expect this to result in increased confidence and trust for UK consumers who engage with these firms.

124. We discuss each of these benefits, how we expect them to materialise for consumers and our approach to estimating their value below.

Reduced financial crime and sanctions evasion

125. We expect our intervention to reduce the incidence of financial crime (including fraud, scams, money laundering, terrorist and proliferation financing), in UK cryptoasset markets. Financial crime and sanctions evasion create significant damage to society, though undermining market integrity and reducing consumers' and market participants' confidence. Reducing financial crime will result in significant society-wide benefits

126. Financial crime includes frauds and scams, with our consumer survey data estimated 9% of current cryptoasset owners had personally been a victim of a cryptoasset fraud or scam, of which 90% indicated they had lost money as a result. While our survey data did not specify a time period for when scams had occurred, extrapolating this data across the population of UK adults who own cryptoassets suggest over 565,000 UK adults have at some point lost money due to a cryptoasset scam or fraud.

127. By applying Financial Crime sourcebooks and guides (FCG and FCTR) to cryptoasset firms, establishing conduct requirements for Senior Managers, and introducing high-level standards to cryptoasset firms, we are looking to ensure only legitimate businesses can operate in UK cryptoasset markets. To estimate the benefits of reduced scams, we use data from Investment products to estimate the impact of our intervention.

128. Action Fraud data indicates an estimated 17,000 crypto-related scams in 2024¹¹. In comparison there were around 8,900 scams related to other Investment products, which are currently regulated. To estimate the annual number of cryptoasset scams after our regulation comes into force, we adjust the Investments figure to reflect the smaller market size of cryptoassets.

129. We assume that the number of cryptoasset scams will gradually fall in the first five years after the implementation of our new policies. After five years, we predict that the effects of the new regime will stabilise. We adjust our figures to reflect our prediction that, in the first five years of the policy, the size of the cryptoasset market will be increasing.

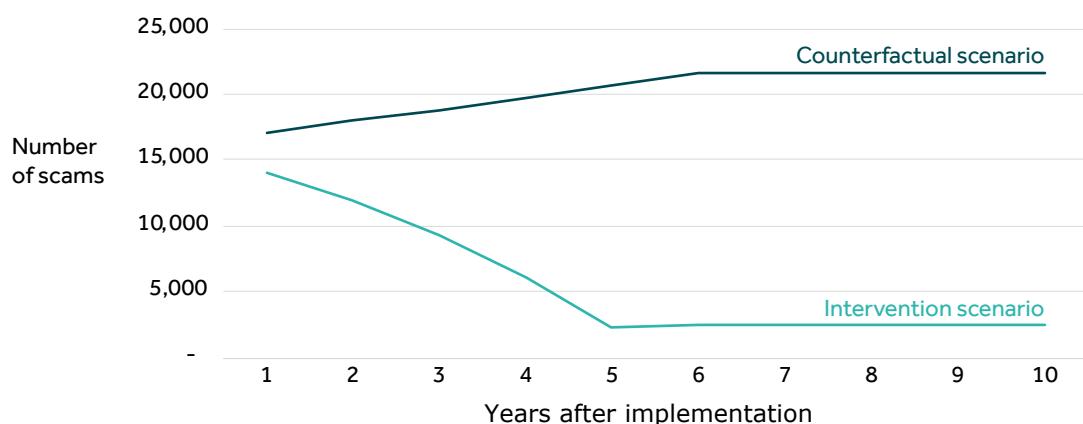
¹¹ FLS survey data suggests 300,000 adults affected by cryptoasset scams in 2024. Not all scams will be reported (of all instances of fraud/ scams, FLS data suggests only 13% reported to Action Fraud).

130. To quantify the benefits of reduced fraud and scams, we require an estimate of the average amount lost currently to cryptoasset scams, and how we expect this to change following our intervention. We have several data sources on the average amount lost to cryptoasset scams:

- Our consumer research, suggests most consumers lost less £500 in a cryptoasset scam, with 20% suggesting they lost over £1,000 (24% of respondents did not provide an answer to this question).
- Data published by Lloyds, indicates the average amount lost in cryptoasset scams was over £10,000 in 2023, up from £3,000 in 2022. Note not all scams will have involved individuals who currently own cryptoassets.

131. To account for this range, we assume the average amount lost to scams that will be prevented by our intervention is £1,000. We believe this represents a reasonable assumption given the variance in volumes we have observed, while recognising that our intervention will not entirely prevent fraud and scams in cryptoasset markets. We assume this figure remains constant throughout the 10-year appraisal period, proportional with changes in consumer demand.

Figure 11 – Anticipated number of cryptoasset scams with/ without our intervention



132. In total, we estimate £130m benefits NPV from frauds and scams due to our proposed intervention, with an average annual undiscounted benefit of £16m.

Increased trust and regulatory certainty

133. In the absence of clear guidance and regulation from the FCA, consumers are likely to be unsure of their rights. For example, our Financial Lives Survey found that many current cryptoasset holders believe they have levels of regulatory protections equivalent to other FSMA-authorised firms.

134. By publishing clear standards, we will standardise rights across different firms and reduce uncertainty for consumers. This will enable more consumers to take advantage of protections offered to them and help them to make better-informed decisions about investments.

Benefits to firms

135. We expect our new regime to have additional benefits for firms. While we do not quantify these, we anticipate they will have a monetary value, through allowing for improved firm efficiency and decision-making. These benefits include:

- **Enhanced regulatory clarity:** Our intervention will clarify standards, provide guidance, and reduce speculation over future regulatory actions, leading to lower uncertainty.
- **Reduced risk aversion from wider financial sector:** By applying Handbook rules to cryptoasset firms, we expect our regulation will enhance credibility within the UK cryptoasset market. This may increase engagement with non-cryptoasset firms and alleviate challenges some cryptoasset firms have raised in accessing banking services.
- **Greater consumer trust:** Our requirements around transparency, operational resilience, and governance will increase consumer confidence in firms, potentially leading to higher demand for cryptoasset products.
- **Greater operational resilience:** Our operational resilience standards will support firms in better managing the impact of operational disruptions. This will provide benefits to both firms and consumers, with firms more aware of their risks and better able to mitigate against them.

Costs

Cost to firms

136. Costs will be both one-off (associated with implementation of our requirements) and ongoing (which firms will incur in order to be compliant with our rules). As noted previously, the cost estimates below are subject to reporting inaccuracies and small sample size bias of our survey data.

Firm Standards: Systems and Controls

137. Our proposed rules will require firms to comply with Senior Managers, Systems and Controls (SYSC) Sourcebook. SYSC requires firms ensure their employees have the appropriate knowledge and competence to perform their roles. This will primarily include:

- Senior Managers and Certification Regime
- Financial Crime
- Operational Resilience

Senior Managers and Certification Regime requirements

138. The Senior Managers Regime imposes high standards to the most senior people in the firm who perform key roles. The key aims of our Senior Managers rules are to:

- Promote staff to take personal responsibility for their actions
- Improve conduct at all levels
- Create clear accountability, ensuring firms and staff clearly understand and can demonstrate roles and functions within the firm

139. The Certification Regime relates to specific roles that are not Senior Manager Functions but can have a significant impact on customers, markets and the risk profile of the firm. Firms are required to certify the fitness and propriety of employees who perform these roles. Staff need to be assessed and issued with a certificate by the firm on appointment and annually thereafter.

140. For our CBA, we assume all firms are classed as core, although we recognise that there may be a very small number who are subsequently classed as enhanced, depending where the threshold for enhanced SMCR is set, as discussed in Chapter 3. Firms will incur one-off familiarisation costs associated with SM&CR rules, in addition to ongoing training and reporting costs. Firms may also need to implement business model and organisational structure changes to comply with SM&CR rules, which may result in additional IT and governance costs. We estimate the total size of these one-off costs to average £19k per firm.

141. Ongoing costs which relate to compliance with the SM&CR rules, including staff training and engagement with the FCA are estimated at £7k per firm.

Financial Crime rules

142. All authorised firms will be required to comply with our financial crime requirements, which can be found in the FCA Handbook under SYSC 6 and the MLRs, and will need to read relevant guidance associated with this, such as the Financial Crime Guide (FCG) and the Financial Crime Thematic Reviews (FTCR). The requirements under SYSC 6 and FCG are broader than those contained in the MLRs, covering anti-bribery and corruption, sanctions, fraud, and other aspects of financial crime.

143. We expect all cryptoasset firms to face one-off familiarisation costs as they work to understand the requirements set out within our financial crime rules and guidance. We assume 280 pages of reading will be required, including legal text review of good and bad practice (as set out in the FCG).

144. We expect some firms will undertake business model changes to comply with our financial crime rules and guidance. We assume that this would involve a change in firm governance processes, subject to their board approval. In line with our CP24/9 estimate, we assume 5% of firms will be required to undertake these changes, spread evenly across our firm population.

145. Any firms regulated within the FCA's cryptoasset regime will first be assessed for the financial crime handling at their application stage. We assume only firms with robust approaches to financial crime prevention will be authorised and within our firm population. We assume firms which have poor approaches to financial crime prevention will not be approved at the authorisation stage, and so not be within our firm population that undertakes a change project.

146. Total one-off costs to firms are estimated at £2.6m, with includes familiarisation with rules and undertaking necessary business model changes to ensure compliance. Following necessary business model changes, we do not anticipate any incremental ongoing costs to firms associated with our financial crime rules.

Operation Resilience

147. Firms will be brought into alignment with our operational resilience requirements through our existing requirements under SYSC 15A. Operational resilience is the ability of firms to prevent, adapt, respond to, recover and learn from operational disruptions. Through introducing and applying these requirements to cryptoasset firms, our aim is to improve the resilience of the sector and reduce consumer harm associated with operational disruptions.

148. Firms will incur familiarisation costs associated with introducing these systems and requirements. We have estimated the costs of this to firms based on the time required to read the 28 pages within the Handbook and non-handbook guidance. Following familiarisation with our proposals, we expect firms to conduct a legal review and gap analysis to check their current practices against the FCA expectations, which will result in additional costs to firms.

149. In addition to organisational changes, cryptoasset firms may need to adjust their IT systems to become compliant with our rules. We also anticipate ongoing IT maintenance costs including not only the purchase or renting of hardware, but also staff and other costs associated with project management, programming, design and analysis.

150. One-off implementation costs of these proposals are estimated at £61k average per firm, with ongoing costs of £23k.

Total SYSC costs

151. Costs associated with Applying SYSC sourcebooks to cryptoasset firms are outlined in the table below:

SYSC Area	Regulatory Requirement	Transition Costs (average per firm)	Transition Costs (population)	Ongoing Costs (per firm)	Ongoing Costs (population)	Total population cost (PV across 10 year appraisal period)
Senior Managers	Senior Manager Rules	£12k	£2.1m	£4k	£0.8m	£5.8m
	Certification Regime	£4k	£0.7m	£2k	£0.4m	£2.5m
	Conduct Rules	£3k	£0.6m	£1k	£0.2m	£1.5m
	Total SM&CR costs	£19k	£3.3m	£7k	£1.3m	£9.8m
Financial Crime	Familiarisation	£7k	£1.3m	£0	£0	£1.2m
	Business model changes	£9k	£1.5m	£0	£0	£1.4m
	Total FC compliance costs	£16k	£2.9m	£0	£0	£2.6m
Operational Resilience	Familiarisation	£39k	£6.6m	£10k	£2.9m	£19.3m
	Training costs	£5k	£0.9m	£6k	£0.7m	£7.9m
	IT costs	£18k	£3.3m	£7k	£1.2m	£11.9m
	Reporting Operational Disruptions	£0	£0	~£1k	£0.1m	£0.1m
	Total Operational Resilience costs to firms	£61k	£10.8m	£23k	£4.8m	£39.1m
Total SYSC		£94k	£17.1m	£31k	£7.4m	£51.6m

152. There may be additional costs associated with SYSC which are not captured above. For example, the increased accountability for Senior Managers may deter certain individuals from taking on senior roles due to the increased responsibility. This could have the unintended effect of deterring risk-averse individuals from seeking these positions, increasing risk-taking by firms, or deter Senior Managers from making innovative decisions if they face greater scrutiny.

153. In addition, many cryptoasset firms would likely incur significant costs if they were to comply with our financial crime rules, due to the nature of their business models. We account for this through our assumptions on firm population and also anticipate it will be reflected in HMT's IA bringing cryptoasset activities within our regulatory framework.

While financial crime costs capture one-off sourcebook and guidance familiarisation, we recognise for many cryptoasset firms, financial crime compliance will result in significant ongoing costs.

High Level Standards

154. Our High Level Standards and Principles for Businesses (PRIN) are fundamental obligations all authorised firms must adhere to. These principles are designed to ensure firms act with integrity, treat customers fairly, and maintain proper standards of conduct. These represent a general statement of the fundamental obligations we expect cryptoasset firms to comply with.

155. Firms will need to familiarise themselves with the rules and guidance that form our High-Level Standards. This comprises sections from PRIN, COCON, FIT, and GEN from the FCA Handbook. This results in 306 pages for familiarisation for firms. Firms will also be required conduct a gap analysis. We estimate an average one-off cost from applying our High-Level Standards to firms of £6k. We do not anticipate any ongoing costs.

Regulatory Requirement	Transition Costs (average per firm)	Transition Costs (population)	Ongoing Costs (per firm)	Ongoing Costs (population)	Total population cost (PV across 10 year appraisal period)
<i>PRIN familiarisation</i>	£6k	£1.1m	£0	£0	£1.1m
Total PRIN costs to firms	£6k	£1.1m	£0	£0	£1.1m

Additional requirements for cryptoasset custodians

156. In CP25/14 (stablecoin issuance and cryptoasset custody), we consulted on proposed rules that would apply to cryptoasset custodians. In this CP, we are proposing additional requirements for cryptoasset custodians, which include:

- **Providing client statements:** Custodians will be required to provide disclosures to clients about their safeguarding arrangements. This will include how certain arrangements may give rise to specific consequences or risks for those client assets.
- **Appointing an external auditor:** custodians will be required to provide us with an annual audit, carried out by an independent external auditor.
- **Appointing a CASS oversight officer:** Custodians must appoint an individual accountable for overseeing the custody arrangements, including reviewing processes and controls, and oversight of third-party providers.

157. These requirements will only apply to firms providing cryptoasset custody services to UK consumers and so only affect a subsample of our regulated cryptoasset population. In CP25/14, we estimated 50 firms would provide cryptoasset custody services.

Based on responses to our custodian's survey, we estimate these one-off costs to average £65k per firm, with ongoing costs of £130k.

Regulatory Requirement	Transition Costs (average per firm)	Transition Costs (population))	Ongoing Costs (per firm)	Ongoing Costs (population)	Total population cost (PV across 10 year appraisal period)
<i>Providing Client Statements</i>	£11k	£540k	£12k	£560k	£3.9m
<i>Appointing an external auditor</i>	£11k	£560k	£31k	£1.5m	£9.7m
<i>CASS Oversight officer</i>	£43k	£2.1m	£85k	£4.2m	£26.6m
Total additional CASS costs to firms	£65k	£3.2m	£130k	£6.2m	£40.2m

Total costs to firms

158. In the below table, we aggregate the estimated costs applying our existing Handbook rules to cryptoasset firms that will be in scope of FCA regulation once we introduce our proposed regime.

Regulatory Requirement	Transition Costs (per firm)	Transition Costs (population))	Ongoing Costs (per firm)	Ongoing Costs (population)	Total population cost (PV across 10 year appraisal period)
<i>Senior Managers and Certification Regime</i>	£19k	£3.3m	£8k	£1.3m	£9.8m
<i>Financial Crime rules and guidance</i>	£15k	£2.9m	£0	£0	£2.6m
<i>Operational Resilience</i>	£60k	£10.8m	£23k	£4.8m	£39.1m
<i>High Level Standards (PRIN)</i>	£6k	£1.1m	£0	£0	£1.1m
<i>Additional requirements for cryptoasset custodians</i>	£65k	£3.2m	£130k	£6.4m	£40.2m
Total Costs	£165k	£21.5m	£160k	£13.8m	£92.6m

159. Average costs for firms are estimated at £100k of implementation costs to become compliant with our rules. We anticipate firms will then incur average ongoing annual costs of £30k. For firms conducting custody of cryptoasset activities, there will be additional one costs of £30k and £130k respectively. Across our 10-year appraisal period and estimated firm population, this results in a total cost with a net present value of £164m for our proposals.

160. These cost estimates primarily relate to compliance costs that will be incurred by firms. There will likely be additional costs to firms associated with changes in business models which we have not captured above. New requirements could force companies to exit the market if they cannot meet the costs of our requirements, which may involve wind-up costs or stranded assets.

Costs to consumers

161. Firm may pass on their additional costs to consumers through higher prices. This may be exacerbated if our intervention raises barriers to entry and reduces competition in the market. If firms cannot pass through costs, it may lead to them cutting operating costs by reducing the quality of their offering, which would also impact consumers. Alternatively, firms could reduce their spending on Research and Development, which could negatively impact innovation.

162. There is also a risk that because of the increased consumer protection under the new regime, consumers will assume that they have protection in areas they do not. This halo effect of regulation could result in consumers purchasing products which they would not do otherwise. This could involve consumers believing, they have greater levels of regulatory protection than they do (i.e. FSCS protection) or that regulation will protect price levels of cryptoassets or reduce market

163. We will take measures to address and minimise the above costs to consumers. We will ensure our communication is clear, to help consumers understand the regulatory protection our regime provides. However, costs may still materialise to consumers and while we do not consider it reasonably practicable to estimate these costs, we recognise they may be significant for some consumers.

Costs to the FCA

164. We will incur costs for authorising firms in the new regime. The average time a case officer spends on one firm is around 40 hours, although that number can vary significantly with the size of the firm. We will recover these costs from firms through charging authorisation fees (which could be passed on to consumers).

165. There will also be costs associated with supervising additional firms and familiarisation with new and emerging business models. Costs could materialise from communication and publication of new rules. The FCA may incur additional costs to review monthly safeguarding returns and auditors' safeguarding reports.

Risks and uncertainty

166. Due to the novel and emergent nature of cryptoasset markets, our analysis is highly sensitive to our key assumptions and there is a high degree of intrinsic uncertainty around its evolution. If our assumptions do not hold or if we have not accounted for all market dynamics, the costs and benefits discussed in this CBA may be over or understated. in addition, data challenges and limitations in our methodologies could lead to inaccuracies in our estimates.

167. To better account for this intrinsic uncertainty we have undertaken additional analysis examining a scenario where our regulatory intervention is less effective at achieving our intended outcomes, than assumed in our central scenario. There are several factors which could result in this being the case, including:

- Criminals and other bad actors adapting to our rules, which could result in our intervention being less effective at preventing financial crime
- Challenges associated with unregulated cryptoasset firms becoming compliant with our rules, resulting in higher compliance costs.
- Regulatory "leakage", with consumers shifting their demand to non-FCA regulated cryptoasset firms overseas.

168. To analyses this scenario, we make the following changes to our assumptions: across several key assumptions, including:

- **Lower reduction in fraud and scams:** Through applying Handbook rules, we anticipate firms will take greater action to reduce frauds and scams in UK cryptoasset markets. However, criminals may adjust to our rules or shift to alternative methods, and so the effective reduction in frauds and scams may be lower than estimated in our central scenario.
- **Higher compliance costs:** Our cost estimates are based on a combination of survey responses, previous CBAs and our Standardised Cost Model. However, costs incurred per firm may be higher if currently unregulated firms need more time to adjust to our proposed rules.

169. For both the above, we consider both a moderate and a more substantial reduction in the effectiveness of our intervention, which we model through adjustments to our assumptions:

- **"Moderately reduced effectiveness" scenario:** Reduction in amount lost to scams 25% lower relative to central estimates.
- **"Substantial reduced effectiveness" scenario:** Compliance costs 25% higher and reduction in amount lost to scams 25% lower relative to central estimates.

170. Results of our analysis are provided in the table below.

	PV Benefits	PV Costs	NPV
Central Estimate	£130m	£92.6m	+£37m
Moderate Scenario	£97.5m	£92.6m	+£4m
Substantial Scenario	£97.5m	£115.7m	-£18m

171. Overall, our sensitivity analysis suggests the net benefit of our intervention is reasonably robust to a moderate reduction in its assumed effectiveness, delivering a marginally positive NPV. This suggests that even if our intervention is less effective at reducing financial crime than anticipated, quantified benefits still exceed quantified costs

172. In our “substantially reduced effectiveness” scenario, our intervention delivers a negative NPV, with quantified costs to firms outweighing the estimated benefits from reduced frauds and scams. This scenario reflects us significantly underestimating costs to firms, in addition to our intervention being less effective at reducing frauds and scams. However, this does not account for additional benefits we have not quantified but would likely materialise from our intervention, such as improved regulatory clarity for firms and consumers. It also does not include costs which could occur in our baseline if we did not apply Handbook rules to cryptoasset firms (e.g. regulatory arbitrage between the existing financial sector and regulated cryptoasset activities).

173. While recognising the uncertainty, our scenario analysis suggests applying FCA Handbook rules to cryptoasset firms will provide net positive benefits even when subject to small-to-moderate changes to key assumptions, particularly when accounting for non-quantified benefits.

Break-even analysis

174. Our quantified benefits are estimated based on a reduced frequency of frauds and scams in UK cryptoasset markets. Due to the nature of how the supporting evidence for these estimates have been compiled (ie self-reported surveys, comparison with traditional investment products) these estimates should be considered as being subject to a significant degree of uncertainty.

175. We anticipate further benefits will materialise to consumers as a result of our proposed intervention, namely increased trust and confidence within UK cryptoasset markets. To account for the uncertainty and potential value of these non-quantified benefits, we have conducted a breakeven analysis to contextualise the benefits scope of our proposals. This illustrates the benefits that would need to be realised for each UK cryptoasset consumer for the proposed changes to be net beneficial.

176. To estimate the breakeven benefits, we used the total quantified costs that we estimate firms would incur over the 10-year appraisal period, in present value terms (£92.6m). We divided this by the total number of UK consumers we currently engaged, and those who we expect to engage in cryptoasset markets in our counterfactual scenario (8.5m). We estimate the breakeven benefit per year per firm by dividing the breakeven benefit per firm by the number of appraisal years (10 years), discounting future values. We also consider a scenario where costs are 25% higher than anticipated in our central estimates.

177. Results of our breakeven analysis are presented in the table below.

	PV Costs	Breakeven-Point per consumer (10 year)	Breakeven-Point per consumer (annual)
Central Estimate	£92.6m	+£12	+£1.25
25% Higher Cost scenario	£115.7m	+£15	+£1.50

178. Our breakeven analysis suggests that our intervention will be net beneficial to consumers if it provides in excess of £12 of value to each UK cryptoasset consumer over the course of our appraisal period (or £15 in our higher cost scenario). This is equivalent to £1.25 and £1.50 per consumer, per year, respectively. Given UK average cryptoasset portfolios were £1,850 as of August 2024, and that our research suggests most consumers would welcome additional regulatory protections, we consider it plausible that the benefits from our intervention to consumers will exceed the estimated breakeven threshold.

Competition assessment

179. Our regime aims to reduce consumer harm by establishing clear standards for firms. While necessary to reduce consumer harm, these regulatory requirements can act as barriers to entries for firms, which may limit competition in the market. We recognise this trade-off between competition and consumer protection, and that our intervention may result in lower levels of competition in UK cryptoasset markets than if we introduced lower standards for firms.

180. Competition in the market may be negatively affected due to:

- Firm exit and reduced product offerings, as a result of higher regulatory standards.
- Prospective entrants to the cryptoasset market facing higher barriers to entry due to increased regulatory costs and reduced prospective profits.
- The ability of larger firms to more easily absorb increased compliance than smaller firms.
- Potentially higher standards applied to UK cryptoasset firms and overseas firms, which may affect UK firms ability to compete in international cryptoasset markets.

181. The combined negative effects on competition of the above could ultimately result in increased prices, reduced quality and lower levels of innovation.

182. We consider that the negative effects on competition and consumer outcomes could be mitigated by several factors:

- Proposals such as applying our High-Level Standards should improve clarity and reduce risk to consumers who choose to shop around in the market. Introducing common standards across regulated firms may reduce risks to consumers from moving to smaller platforms and encourage firms to compete on price and product quality more than they currently do.

- Increased regulatory protections are anticipated to increase demand for cryptoasset products. This may offset the effect of higher compliance costs to firms and encourage greater entry to the market.

183. We will monitor the impact of our intervention on the degree of competition in UK cryptoasset markets. We anticipate that the aggregate effect on competition over our appraisal period will be positive, with the initial increase to barriers to entry being offset by increased firm entry and consumer demand.

Wider economic impacts, including on secondary objective

184. Our proposals will help to support competitiveness and growth in the UK through influencing four of our seven drivers:

- **Innovation:** Our regulation provides greater clarity and legitimacy to cryptoasset firms. This creates an environment for increased innovation within UK financial services, benefitting competitiveness and growth.
- **Proportionate regulation:** Through relying on rules-based outcomes our intervention looks to reduce harm while providing flexibility to firms to innovate and without being overly costly or burdensome to firms. This will allow firms located within the UK to compete with international firms and improve the UK's competitiveness as a financial hub.
- **Market stability:** By introducing operational resilience standards for cryptoasset firm, we reduce the likelihood of market disruption and system contagion. Protecting consumers and firms in this way builds confidence in UK institutions and provides a foundation for increasing investment in the UK, which, supports productivity and market growth.
- **International markets:** Our rules have been designed to be consistent with international peers, following recommendations for regulation of cryptoassets published by IOSCO. This will ensure the UK is an attractiveness place for cryptoasset firms to invest and for businesses to establish or raise capital.

185. We anticipate the standards we introduce will support UK competitiveness through clear standards and robust regulation. We recognise an interaction between developing a cryptoassets regime that protects consumers and supports market integrity, and the resulting impact on growth. Consumer protection and market integrity build trust and participation, which increase trust and growth. However, disproportionate requirements could make adversely impact competition and firm costs and potentially inhibit growth.

186. From our review of the relevant literature, we did not identify evidence to suggest economic growth materialising from consumers purchasing cryptoassets. Any benefits would instead be due to consumers increasing their consumption from converting gains in cryptoasset holdings to increased income, which we anticipate as being limited. 250. Growth may also materialise due to increased exports (i.e. if UK based cryptoasset firms attract business from overseas customers).

187. We see the impact of our intervention on economic growth as dependent on the cryptoasset sector interlinking with, and creating benefits in, the real economy. We identify 3 key ways in which cryptoassets could benefit the UK's growth objective:

- **Labour market impacts:** Cryptoasset firms employ high-skilled workers and our intervention could attract cryptoasset firms to establish in the UK. This would result in direct jobs (and supporting supply chain jobs) and potentially higher wages for those in the industry. We assess the potential impact on growth to be small, due to low jobs numbers, meaning any new jobs would have small impact on growth.
- **Capital Inflows and Liquidity:** Similarly, more cryptoasset firms located in the UK could result in capital inflows. Higher liquidity could in turn increase efficiencies in the UK's financial sector which could impact growth.
- **Innovation:** Increased use of cryptoassets and DLT due to more consumer confidence and trust may result in new products and services, benefiting consumers across the economy. Innovation is a core driver of economic growth, but the impact on growth is contingent on how the rest of economy uses cryptoasset technology (directly or indirectly).

188. Our assessment suggests potential for our intervention to improve international competitiveness and growth in the medium-to-long term through the above factors. However, this is subject to a significant uncertainty and dependent on the extent to which cryptoasset firms establish in the UK. Growth is also dependent on several exogenous variables, in particular, the ability of DLT to create efficiencies at scale and compete with legacy financial infrastructure. However, based on the size of UK cryptoasset market currently (which has few UK-based firms), we think our intervention will not adversely impact UK economic growth, while creating opportunities for growth in the future.

Monitoring and evaluation

189. As outlined in our causal chain, we anticipate our intervention will result in reduced harm to consumers who choose to engage with cryptoassets. We also expect our outcomes-based regulation will reduce uncertainty to firms and increase competition and the UK's competitiveness in the cryptoasset sector.

190. We intend to measure the effectiveness of our interventions through:

- Regulatory returns information submitted to the FCA by cryptoasset firms as part of their regulatory requirements.
- Survey data, including our Consumer Research series and FLS. These will allow us to track changes in attitudes, behaviour, and demand.
- Monitoring competition within UK cryptoasset markets.

Consumer outcomes

191. We expect our rules to reduce consumer harm from their involvement in cryptoasset markets, through reduced scams, greater awareness, and enhanced protections.

Through our intervention, we expect that consumers will be better informed to make appropriate investment decisions.

192. We will monitor this through our consumer research series, which includes measures of the following:

- Understanding of products
- Scams, losses, and other negative experiences
- Awareness of regulation and understanding of risks

Firm outcomes

193. We expect our regulation will result in reduced uncertainty for firms. It may also increase demand for cryptoassets, as consumer confidence increases.

194. To monitor the effect of these standards on firms, we will continue to gather information on the market. We will engage with firms to identify challenges to regulation and any improvements to enhance proportionality and appropriateness.

Consultation with the FCA Cost Benefit Analysis Panel

195. We have consulted the CBA Panel in the preparation of this CBA in line with the requirements of s138IA(2)(a) FSMA. A summary of the main group of recommendations provided by the CBA Panel and the measures we took in response to Panel advice is provided in the table below. In addition, we have undertaken further changes based on wider feedback from the CBA Panel on specific points of the CBA. The CBA Panel publishes a summary of their feedback on their website, which can be accessed [here](#).

CBA Panel Main Recommendations	Our Response
Clarify basic rationale for extension of conduct regulation perimeter. Given the extensive evidential and analytical base underpinning the UK's existing conduct regulation regime for traditional financial products, the broad outlines of the rationale for extending the perimeter to cryptoasset activities is unlikely to be controversial. Nevertheless, the Panel recommends that the CBA should present more clearly the economic case for applying conduct regulation to cryptoasset activities, explaining in particular how it relates to (i) the HM Treasury's draft Statutory Instrument and its Impact Assessment; (ii) the existing base of CBA supporting conduct regulation for traditional financial services; and (iii) the principle of ensuring a level regulatory playing-field between traditional financial and cryptoasset services.	We have provided additional evidence outlining our rationale for intervention relating to conduct, including: <ul style="list-style-type: none">• How and why the market failures identified currently arise in UK cryptoasset markets• How the specific elements of our intervention will address and account for these market failures• How our proposed intervention supports a level playing field between cryptoasset firms and traditional financial firms, and is technology agnostic

CBA Panel Main Recommendations	Our Response
<p>Clarify conceptualisation of market for cryptoasset services and focus analysis on areas of divergence from traditional financial services. The markets for cryptoasset and traditional financial services also differ significantly in several respects which make the existing analytical base for regulation less transferable. For example, there are distinctive issues relating to (i) jurisdiction – such as the current dominance of the UK market by a large, existing universe of offshore service providers; and the importance of entities of indeterminate jurisdiction, such as permissionless Distributed Ledger Technologies (DLTs) – and (ii) functional diversity – such as the role of certain cryptoassets as both investment products and payments media. The Panel therefore recommends that the CBA focus its analysis on how these divergent features of cryptoasset markets will affect the impact of the proposed regime.</p>	<p>We have provided further detail on jurisdictional issues and differences between Cryptoasset products and other FSMA regulated products, and how we have accounted for this within our analysis. This has included discussion and consideration of permissionless DLT, and how their use can result in different operational risks and challenges for cryptoasset firms. We have also highlighted the different use cases for cryptoassets and how we account for this within our analysis (while noting our survey data indicates most UK consumers currently consider them an investment product).</p>
<p>Sharpen analysis of proposed regulatory disparities between traditional and cryptoasset, and on- and offshore, providers on the market and wider economy. The proposed intervention implies a level playing field between traditional and cryptoasset service providers in many areas, but not in some important ones. The Panel recommends that the CBA is more explicit in its analysis of the economic impacts of these differences – including dynamic impacts such as migration by consumers and potential regulatory arbitrage by service providers.</p>	<p>We have provided additional analysis on these disparities and how they may impact market dynamics.</p> <p>In terms of wider regulatory arbitrage, we have referenced this throughout our CBA, we anticipate forthcoming FCA Cryptoasset CBAs will be better able to account for these risks and impacts. In particular, our CBA which will accompany rules for Trading Platforms and Intermediaries (which are how the vast majority of UK consumers engage with cryptoasset markets) will include a detailed consideration of these risks and trade-offs.</p>

Question 28: Do you agree with our assumptions and findings as set out in this CBA on the relative costs and benefits of the proposals contained in this consultation paper? Please give your reasons.

Question 29: Do you have any views on the cost benefit analysis, including our analysis of costs and benefits to consumers, firms and the market?

Annex 3

Compatibility statement

Compliance with legal requirements

- 1.** This Annex records the FCA's compliance with a number of legal requirements applicable to the proposals in this consultation, including an explanation of the FCA's reasons for concluding that our proposals in this consultation are compatible with certain requirements under the Financial Services and Markets Act 2000 (FSMA).
- 2.** When consulting on new rules, the FCA is required by section 138I(2)(d) FSMA to include an explanation of why it believes making the proposed rules (a) is compatible with its general duty under section 1B(1) FSMA, so far as reasonably possible, to act in a way which is compatible with its strategic objective and advances one or more of its operational objectives, (b) so far as reasonably possible, advances the secondary international competitiveness and growth objective, under section 1B (4A) FSMA, and (c) complies with its general duty under section 1B(5)(a) FSMA to have regard to the regulatory principles in section 3B FSMA. The FCA is also required by s 138K(2) FSMA to state its opinion on whether the proposed rules will have a significantly different impact on mutual societies as opposed to other authorised persons.
- 3.** This Annex also sets out the FCA's view of how the proposed rules are compatible with the duty on the FCA to discharge its general functions (which include rule-making) in a way which promotes effective competition in the interests of consumers (section 1B(4)). This duty applies in so far as promoting competition is compatible with advancing the FCA's consumer protection and/or integrity objectives.
- 4.** In addition, this Annex explains how we have considered the recommendations made by the Treasury under s 1JA FSMA about aspects of the economic policy of His Majesty's Government to which we should have regard in connection with our general duties.
- 5.** This Annex includes our assessment of the equality and diversity implications of these proposals.
- 6.** Under the Legislative and Regulatory Reform Act 2006 (LRRA) the FCA is subject to requirements to have regard to a number of high-level 'Principles' in the exercise of some of our regulatory functions and to have regard to a 'Regulators' Code' when determining general policies and principles and giving general guidance (but not when exercising other legislative functions like making rules). This Annex sets out how we have complied with requirements under the LRRA.

The FCA's objectives and regulatory principles: Compatibility statement

7. The proposals set out in this consultation paper are primarily intended to advance the FCA's operational objectives of:

- Delivering consumer protection- securing an appropriate degree of protection for consumers
- Enhancing market integrity – protecting and enhancing the integrity of the UK financial system
- Building competitive markets – promoting effective competition in the interests of consumers.

8. We consider that, so far as possible, these proposals advance the FCA's secondary international competitiveness and growth objective by improving confidence in the UK as a place where cryptoasset activities can be carried out in a trusted market with clear and proportionate requirements. Our proposals for firms on High-level Standards, Governance, Senior Managers & Certification Regime (SM&CR), Operational Resilience and Financial Crime intend to ensure that the UK remains a suitable and stable environment and destination for doing business. We have also had regard to relevant international standards set by bodies including the Financial Stability Board and IOSCO, both of which the FCA played a role in developing.

9. In preparing the proposals set out in this CP, the FCA has had regard to the regulatory principles set out in s 3B FSMA.

The need to use our resources in the most efficient and economic way

10. These proposals will help us to improve our supervisory oversight of cryptoasset businesses. We are consulting on High Level Standards which are core principles that define the fundamental obligations that apply to all FCA-authorised firms. These standards are intended to ensure that firms have higher governance standards, greater Senior Management accountability, and more robust Operational Resilience plans, amongst other changes. By ensuring that firms can meet our standards before receiving authorisation, our proposals are intended to reduce the need for supervisory interventions.

The principle that a burden or restriction should be proportionate to the benefits

11. We have carefully considered the proportionality of our proposals, including through consultation with internal stakeholders through the development of our proposals.

12. The proposals may require firms to make changes, with associated costs, as to how they conduct their business. However, we consider that our proposals are proportionate, and the benefits outweigh the costs. The CBA in Annex 2 sets out the costs and benefits of our proposals.

The need to contribute towards achieving compliance by the Secretary of State with section 1 of the Climate Change Act 2008 (UK net zero emission target) and section 5 of the Environment Act 2021 (environmental targets)

13. In Chapter 5, we proposed the application of certain rules within the ESG Sourcebook to Cryptoasset Firms. This will require Cryptoasset Firms to ensure that their sustainability claims are fair, clear, and not misleading (ESG 4.3.1R) and that they do not use a sustainability label unless they are asset managers meeting the relevant conditions (ESG 4.1.1R). While these are important sustainability-related protections, we do not consider that these provisions will contribute towards achieving compliance by the Secretary of State with section 1 of the Climate Change Act 2008 (UK net zero emission target) and section 5 of the Environment Act 2021 (environmental targets). Similarly, outside of Chapter 5, we do not consider that there is any contribution the proposals outlined in this consultation can make to these targets.

The general principle that consumers should take responsibility for their decisions

14. Our proposals will provide greater protection for consumers. They do not inhibit consumers' ability to access a range of products, nor do they seek to remove from consumers the need to take responsibility for their own decisions in relation to their use of regulated and unregulated products and services.

The responsibility of senior management

15. Our approach to SM&CR for cryptoasset firms is provided in chapter 3. Our proposals for senior management align with the approach taken by the FCA across all regulated firms, with minimal changes. We are proposing to apply SM&CR, a regime which aims to reduce harm to consumers and strengthen market integrity by creating a system that enables firms and regulators to hold people to account. The SM&CR regime is designed to be sufficiently broad to apply across financial sectors.

The desirability of recognising differences in the nature of, and objectives of, businesses carried on by different persons including mutual societies and other kinds of business organisation

16. Our proposals will apply equally to any regulated firm, regardless of whether it is a mutual society. We recognise that firms conducting different types of cryptoasset activities require different approach and rules. Our proposals include activities specific requirements for cryptoasset firms. We are proposing different rules for different activities in the consultation paper.

The desirability of publishing information relating to persons subject to requirements imposed under FSMA, or requiring them to publish information

17. We have had regard to this principle and believe our proposals are compatible with it, including through our proposed rules on the information qualifying cryptoassets should disclose. We may publish data on aggregate trends in the cryptoasset market.

The principle that we should exercise our functions as transparently as possible

18. By explaining the rationale for our proposals and the anticipated outcomes, we have had regard to this principle.

In formulating these proposals, the FCA has had regards to the importance of taking action intended to minimise the extent to which it is possible for a business carried on (i) by an authorised person or a recognised investment exchange; or (ii) in contravention of the general prohibition, to be used for a purpose connected with financial crime (as required by s 1B(5)(b) FSMA).

19. Our CP proposals are intended to support firms to act as a strong line of defence against financial crime.

Expected effect on mutual societies

20. The FCA does not expect the proposals in this paper to have significantly different impact on mutual societies. Our proposals will apply equally to any regulated firm, regardless of whether it is a mutual society.

Compatibility with the duty to promote effective competition in the interests of consumers

21. In preparing the proposals as set out in this consultation, we have had regard to the FCA's duty to promote effective competition in the interests of consumers.

Equality and diversity

22. We are required under the Equality Act 2010 in exercising our functions to 'have due regard' to the need to eliminate discrimination, harassment, victimisation and any other conduct prohibited by or under the Act, advance equality of opportunity between persons who share a relevant protected characteristic and those who do not, to and foster good relations between people who share a protected characteristics and those who do not.

23. As part of this, we ensure the equality and diversity implications of any new policy proposals are considered. The outcome of our consideration in relation to these matters in this case is stated in our Equality Impact Assessment.

Legislative and Regulatory Reform Act 2006 (LRRA)

24. We have had regard to the principles in the LRRA and Regulators' Code (together the 'Principles') for the parts of the proposals that consist of general policies, principles or guidance. We consider that these parts of our proposals are compliant with the five LRRA principles- that regulatory activities should be carried out in a way which is transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed.

- **Transparent** – We are consulting on our policy proposals with industry to articulate changes. Through consultation and pro-active engagement both before and during consultation, we are being transparent and providing a simple and straightforward way to engage with the regulated community.
- **Accountable** – We are consulting on proposals and will publish final rules after considering all feedback received in our Policy Statement in 2026 as per the Crypto Roadmap. We are acting within our statutory powers, rules and processes.
- **Proportionate** – We recognise that firms may be required to make changes to how they carry out their business and have provided for an implementation period to give them time to do so. The CBA sets out further details on the costs and benefits of our proposals.
- **Consistent** – Our approach would apply in a consistent manner across firms carrying out cryptoasset activities.
- **Targeted** – Our proposals will enhance our ability to provide targeted firm engagement and consider how to best deploy our resources.
- **Regulators' Code** – Our proposals are carried out in a way that supports firms to comply and grow through our consideration of their feedback via the CP and refining our proposals where necessary. Our CP, CBA, draft instrument, accompanying annexes, public communications and communications with firms are provided in a simple, straightforward, transparent and clear way to help firms meet their responsibilities.

Annex 4

Abbreviations used in this paper

Abbreviation	Description
A&D	Admissions & Disclosure
AML	Anti-Money Laundering
AUM	Assets Under Management
CASS	Client Assets
CATP	Cryptoasset Trading Platform
CBA	Cost Benefit Analysis
CD	Consumer Duty
CJ	Compulsory Jurisdiction
COBS	Conduct of Business Sourcebook
COCON	Code of Conduct Sourcebook
COND	Threshold Conditions
CP	Consultation Paper
CPF	Counter-Proliferation Financing
CTF	Counter-Terrorist Financing
DIB	Designated Investment Business
DISP	The Dispute Resolution: Complaints Sourcebook
DLT	Distributed Ledger Technology
DP	Discussion Paper
ECP	Eligible Counterparties
ESG	Environmental, Social and Governance

Abbreviation	Description
FATF	Financial Action Task Force
FCG	Financial Crime Guide
FCTR	Financial Crime Thematic Reviews
FIT	Fit and Proper Test
FOS	Financial Ombudsman Services
FSCS	Financial Services Compensation Scheme
FSMA	Financial Services and Markets Act 2000
GEN	General Provisions
HSM	Hardware Security Modules
IOSCO	International Organisation Of Securities Commissions
KYC	Know Your Customer
MARC	Market Abuse Regime for Cryptoassets
MiFID	Markets in Financial Instruments Directive
MLRs	Money Laundering, Terrorist Financing And Transfer Of Funds (Information on the Payer) Regulations 2017
MPC	Multi-Party Computation
MTF	Multilateral Trading Facilities
NCA	National Crime Agency
NRA	National Risk Assessment
PoS	Proof-of-Stake
PoW	Proof-of-Work
PR	Prescribed Responsibility
PRA	Prudential Regulation Authority
PRIN	Principles for Businesses
PROA	Private Right of Action

Abbreviation	Description
PROD	Product Intervention and Product Governance Sourcebook
PS	Policy Statement
RAO	Financial Services and Markets Act 2000 (Regulated Activities) Order 2001
RMMI	Restricted Mass Market Investments
SI	Statutory Instrument
SICGO	Secondary International Competitiveness and Growth
SMCR	Senior Managers and Certification Regime
SMF	Senior Management Function
SUP	Supervision Manual
SYSC	Senior Management Arrangements, Systems and Controls
TC	Training and Competence Sourcebook
VJ	Voluntary Jurisdiction

Appendix 1

Draft Handbook text

CRYPTOASSETS: CONDUCT AND FIRM STANDARDS INSTRUMENT 202X

Powers exercised

A. The Financial Conduct Authority (“the FCA”) makes this instrument in the exercise of the powers and related provisions in or under:

- (1) the following powers and related provisions in the Financial Services and Markets Act 2000 (“the Act”), including as applied by articles 98 and 99 of the Financial Services and Markets Act (Regulated Activities) Order 2000 (as amended by the Financial Services and Markets Act 2000 (Regulated Activities and Miscellaneous Provisions) (Cryptoassets) Order 2025) as applied by paragraph 3 of Schedule 6 to the Payment Services Regulations 2017 (SI 2017/752) (“the PSRs”) and paragraph 2A of Schedule 3 to the Electronic Money Regulations 2011 (SI 2011/99) (“the EMRs”):
 - (a) section 59 (Approval for particular arrangements);
 - (b) section 60 (Applications for approval);
 - (c) section 60A (Vetting of candidates by authorised persons);
 - (d) section 61 (Determination of applications);
 - (e) section 62A (Changes in responsibilities of senior managers);
 - (f) section 63ZA (Variation of senior manager’s approval at request of authorised person);
 - (g) section 63ZD (Statement of policy relating to conditional approval and variation);
 - (h) section 63C (Statement of policy);
 - (i) section 63E (Certification of employees by authorised persons);
 - (j) section 63F (Issuing of certificates);
 - (k) section 64A (Rules of conduct);
 - (l) section 64C (Requirements for authorised persons to notify regulator of disciplinary action);
 - (m) section 69 (Statement of policy).
 - (n) section 137A (The FCA’s general rules);
 - (o) section 137B (FCA general rules: clients’ money, right to rescind etc.);
 - (p) section 137T (General supplementary powers);
 - (q) section 139A (Power of the FCA to give guidance);
 - (r) section 347 (The record of authorised persons etc.); and
 - (s) section 395 (The FCA’s and PRA’s procedures);
- (2) regulation 120 (Guidance) of the PSRs;
- (3) regulation 60 (Guidance) of the EMRs; and
- (4) the other powers and related provisions listed in Schedule 4 (Powers exercised) to the General Provisions of the FCA’s Handbook.

B. The rule-making provisions listed above are specified for the purposes of section 138G(2) (Rule-making instruments) of the Act.

Commencement

C. This instrument comes into force on [date].

Amendments to the Handbook

D. The modules of the FCA's Handbook of rules and guidance listed in column (1) below are amended in accordance with the Annexes to this instrument listed in column (2).

(1)	(2)
Glossary of definitions	Annex A
Principles for Businesses (PRIN)	Annex B
Senior Management Arrangements, Systems and Controls sourcebook (SYSC)	Annex C
General Provisions (GEN)	Annex D
Supervision manual (SUP)	Annex E

[*Editor's note:* The Annexes to this instrument take into account the proposals suggested in the consultation paper 'Stablecoin Issuance and Cryptoasset Custody' (CP25/14) as if they were made final.]

Notes

E. In the Annexes to this instrument, the notes (indicated by "Note:" or "*Editor's note:*") are included for the convenience of readers but do not form part of the legislative text.

Citation

F. This instrument may be cited as the Cryptoassets: Conduct and Firm Standards Instrument 202X.

By order of the Board
[date]

Annex A

Amendments to the Glossary of definitions

In this Annex, underlining indicates new text and striking through indicates deleted text, unless stated otherwise.

Insert the following new definitions in the appropriate alphabetical position. The text is not underlined.

[*Editor's note:* Definitions and legislative references are based on draft provisions published by HM Treasury that will amend the Regulated Activities Order. These references will be updated as required once the legislation amending the Regulated Activities Order is made.]

<i>arranging deals in qualifying cryptoassets</i>	the <i>regulated activity</i> , specified in article [9Z] of the <i>Regulated Activities Order</i> , which is, in summary, making arrangements:
	<ul style="list-style-type: none"> (a) for another <i>person</i> (whether as <i>principal</i> or agent) to <i>buy, sell, or subscribe for or underwrite a qualifying cryptoasset</i>; (b) with a view to a <i>person</i> who participates in the arrangements <i>buying, selling, subscribing for or underwriting qualifying cryptoassets</i> falling within article [9Z(1)], whether as <i>principal</i> or agent.
<i>arranging qualifying cryptoasset staking</i>	the <i>regulated activity</i> , specified in article [9Z7] of the <i>Regulated Activities Order</i> , which is, in summary, making arrangements for <i>qualifying cryptoasset staking</i> .
<i>blockchain validation</i>	(in accordance with article [9Z7] of the <i>Regulated Activities Order</i>): <ul style="list-style-type: none"> (a) the validation of transactions on: <ul style="list-style-type: none"> (i) a blockchain; or (ii) a network that uses distributed ledger technology or other similar technology; and (b) includes proof of stake consensus mechanisms.
<i>dealing in qualifying cryptoassets as agent</i>	the <i>regulated activity</i> , specified in article [9X] of the <i>Regulated Activities Order</i> , which is, in summary, <i>buying, selling, subscribing for or underwriting qualifying cryptoassets as agent</i> .

<i>dealing in qualifying cryptoassets as principal</i>	the <i>regulated activity</i> , specified in article [9U] of the <i>Regulated Activities Order</i> , which is, in summary, <i>buying, selling, subscribing for or underwriting qualifying cryptoassets as principal</i> .
<i>operating a qualifying cryptoasset trading platform</i>	the <i>regulated activity</i> , specified in article [9T] of the <i>Regulated Activities Order</i> , which is, in summary, the operation of a <i>qualifying cryptoasset trading platform</i> .
<i>qualifying cryptoasset activity</i>	any of the following activities, specified in Part II of the <i>Regulated Activities Order</i> (Specified Activities):
	<ul style="list-style-type: none"> (a) <i>issuing qualifying stablecoin</i> in the <i>United Kingdom</i> (article [9N]); (b) <i>safeguarding qualifying cryptoassets</i>; (c) <i>operating a qualifying cryptoasset trading platform</i> (article [9T]); (d) <i>dealing in qualifying cryptoassets as principal</i> ((article [9U]) (but disregarding the exclusion in article [9V] (Absence of holding out etc)); (e) <i>dealing in qualifying cryptoassets as agent</i> (article [9X]); (f) <i>arranging deals in qualifying cryptoassets</i> (article [9Z]); or (g) <i>arranging qualifying cryptoasset staking</i> (article [9Z7]).
<i>qualifying cryptoasset custodian</i>	an <i>authorised person</i> with <i>permission</i> to carry on the <i>regulated activity</i> specified in article [9O(1)(a)] (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets) of the <i>Regulated Activities Order</i> , but only in relation to <i>qualifying cryptoassets</i> .
<i>qualifying cryptoasset firm</i>	a <i>firm</i> with a <i>Part 4A permission</i> which includes a <i>qualifying cryptoasset activity</i> .
<i>qualifying cryptoasset staking</i>	the use of a <i>qualifying cryptoasset</i> in <i>blockchain validation</i> .
<i>qualifying cryptoasset trading platform</i>	(in accordance with article 3(1) of the <i>Regulated Activities Order</i>) a system which brings together or facilitates the bringing together of multiple third-party <i>buying and selling</i> interests in <i>qualifying cryptoassets</i> in a way that results in a contract for the exchange of <i>qualifying cryptoassets</i> for:

- (a) money (including *electronic money*); or
- (b) other *qualifying cryptoassets*.

safeguarding qualifying cryptoassets and relevant specified investment cryptoassets the regulated activity specified in article [9O] (Safeguarding of qualifying cryptoassets and relevant specified investment cryptoassets) of the *Regulated Activities Order*.

Amend the following definitions as shown.

client

...

- (B) in the *FCA Handbook*:

(1) (except in *PROF*, in *MIFIDPRU 5*, in relation to a *credit-related regulated activity*, in relation to *regulated funeral plan activity*, in relation to a *home finance transaction* and, in relation to *insurance risk transformation* and activities directly arising from *insurance risk transformation*, and in relation to *issuing qualifying stablecoin in PRIN and SYSC 15A*) has the meaning given in *COBS 3.2*, that is (in summary and without prejudice to the detailed effect of *COBS 3.2*) a *person* to whom a *firm* provides, intends to provide or has provided a service in the course of carrying on a *regulated activity*, or in the case of *MiFID or equivalent third country business*, an *ancillary service*:

...

...

(12) ...

(13) (in *PRIN and SYSC 15A* in relation to *issuing qualifying stablecoin*):

- (a) *a person to whom a firm provides, intends to provide or has provided a service in the course of carrying on a regulated activity; and*
- (b) *where not otherwise included in (a), the holder of a qualifying stablecoin which is issued by a qualifying stablecoin issuer.*

customer

...

(B) in the *FCA Handbook*:

(1) (except in relation to *SYSC 19F.2, ICOBS, retail premium finance, a credit-related regulated activity, regulated claims management activity, regulated funeral plan activity, regulated pensions dashboard activity, MCOB 3A, an MCD credit agreement, CASS 5, for the purposes of PRIN in relation to MiFID or equivalent third country business; and issuing qualifying stablecoin, DISP 1.1.10-BR, PROD 1.4 and PROD 4*) and in relation to *payment services* and issuing *electronic money* (where not a *regulated activity*) a *client* who is not an *eligible counterparty* for the relevant purposes.

...

(10) ...

(11) (in PRIN in relation to issuing qualifying stablecoin) a client who is not an eligible counterparty for the relevant purpose.

designated investment business any of the following activities, specified in Part II of the *Regulated Activities Order* (Specified Activities), which is carried on by way of business:

...

(t) *establishing, operating or winding up a collective investment scheme;*

(u) *issuing qualifying stablecoin in the United Kingdom (article [9M]);*

(v) *safeguarding qualifying cryptoassets;*

(w) *operating a qualifying cryptoasset trading platform (article [9T]);*

(x) *dealing in qualifying cryptoassets as principal (article [9U]), but disregarding the exclusion in article [9V] (Absence of holding out etc);*

(y) *dealing in qualifying cryptoassets as agent (article [9X]);*

(z) *arranging deals in qualifying cryptoassets (article [9Z]);*

(za) *qualifying cryptoasset staking (article [9Z7]).*

proprietary trading

(in *SYSC 27* (Senior managers and certification regime: (Certification regime) and *COCON*) *dealing in investments as principal* as part of a

business of trading in *specified investments*. For these purposes *dealing in investments as principal* includes:

- (a) any activities that would be included but for the exclusion in Article 15 (Absence of holding out), Article 16 (Dealing in contractually based investments) or, for a *UK AIFM* or *UK UCITS management company*, article 72AA (Managers of UCITS and AIFs) of the *Regulated Activities Order*;
- (b) *dealing in qualifying cryptoassets as principal*;
- (c) *any activities that would be included in (b) but for the exclusion in [article 9V] (Absence of holding out) of the *Regulated Activities Order**;
- (d) *issuing qualifying stablecoin in the United Kingdom; and*
- (e) *operating a qualifying cryptoasset trading platform to the extent that that activity would have fallen into (b) but for the exclusion in article [9Y(3)(b)] of the *Regulated Activities Order**.

[*Editor's note*: The text that is proposed to be inserted as the new limb (B) of the definition of 'qualifying cryptoasset' was proposed as a new definition for 'qualifying cryptoasset' in the consultation paper 'Stablecoin Issuance and Cryptoasset Custody' (CP25/14). The definition of qualifying cryptoasset will be updated as required once the legislation amending the Regulated Activities Order is made.]

qualifying cryptoasset

- (A) (as defined in paragraph 26F (Qualifying cryptoasset) of Schedule 1 to the *Financial Promotion Order*):
- ...
- (B) *the investment specified in article 88F of the *Regulated Activities Order* (Qualifying cryptoassets)*.

[*Editor's note*: The definition of 'qualifying stablecoin' takes into account the proposals and legislative changes suggested in the consultation paper 'Stablecoin Issuance and Cryptoasset Custody' (CP25/14) as if they were made final.]

qualifying stablecoin

- (1) *(in CRYPTO 2 and CASS 16) the specified investment defined in article 88G (Qualifying stablecoin) of the *Regulated Activities Order*, but only including those specified investments which involve a stablecoin referencing a single fiat currency.*
- (2) *(except in CRYPTO 2 and CASS 16) the specified investment defined in article 88G (Qualifying stablecoin) of the *Regulated Activities Order*.*

regulated activity

...

(B) in the *FCA* Handbook: (in accordance with section 22 of the *Act* (Regulated activities)) the activities specified in Part II (Specified activities), Part 3A (Specified activities in relation to information) and Part 3B (Claims management activities in Great Britain) of the *Regulated Activities Order*, which are, in summary:

...

(aa) ...

(ab) issuing qualifying stablecoin in the United Kingdom (article [9M]);

(ac) safeguarding qualifying cryptoassets and relevant specified investment cryptoassets (article [9O]);

(ad) operating a qualifying cryptoasset trading platform (article [9T]);

(ae) dealing in qualifying cryptoassets as principal (article [9U]);

(af) dealing in qualifying cryptoassets as agent (article [9X]);

(ag) arranging deals in qualifying cryptoassets (article [9Z]);

(ah) arranging qualifying cryptoasset staking (article [9Z7]);

...

retail customer

...

(2) (in *PRIN* and *COCON*):

....

(g) where a *firm* carries out activities in relation to an *occupational pension scheme*, any *person* who is not a *client* of the *firm* but who is or would be a beneficiary in relation to *investments* held in that *occupational pension scheme*;

(h) where a *firm* is a qualifying stablecoin issuer, a *customer* who is not a professional client.

...

specified investment (1) any of the following *investments* specified in Part III of the *Regulated Activities Order* (Specified Investments):

...

(p) *rights to or interests in investments* (article 89);

(r) *qualifying cryptoasset* (article 88F);

(s) *qualifying stablecoin* (article 88G).

...

Annex B

Amendments to the Principles for Businesses (PRIN)

In this Annex, underlining indicates new text.

3 Rules about application

3.1 Who?

...

3.1.1.13 R ...

3.1.1.14 R (1) *Principles 6 and 9 do not apply when a firm provides the service of operating a qualifying cryptoasset platform for professional clients.*

(2) *Principles 1, 2, 6 and 9 do not apply to transactions concluded:*

(a) *between the members or participants of; and*

(b) *under the rules governing,*

a qualifying cryptoasset trading platform.

...

3.2 What?

3.2.1A R *PRIN (other than Principle 12 and PRIN 2A) applies with respect to the carrying on of:*

(1) *regulated activities;*

(2) *activities that constitute dealing in investments as principal, disregarding the exclusion in article 15 of the Regulated Activities Order (Absence of holding out etc);*

(2A) *activities that constitute dealing in cryptoassets as principal, disregarding the exclusion in article [9V] of the Regulated Activities Order (Absence of holding out etc);*

...

...

Annex C

Amendments to the Senior Management Arrangements, Systems and Controls sourcebook (SYSC)

In this Annex, underlining indicates new text and striking through indicates deleted text.

1 Application and purpose

...

1 Annex Detailed application of SYSC

1

...

Part 3	Tables summarising the application of the common platform requirements to different types of firm		
...			
3.3A	R	...	
<u>3.4</u>	<u>G</u>	For a <i>qualifying cryptoasset firm</i> that:	
	(1)	<u>is a common platform firm, SYSC 4 to SYSC 10 apply as set out in SYSC 1 Annex 1 3.2G; or</u>	
	(2)	<u>is not a common platform firm and is not subject to MiFID, SYSC 4 to SYSC 10 apply as set out in SYSC 1 Annex 1 3.3R.</u>	

...

15A Operational resilience

15A.1 Application

Application

15A.1.1 R This chapter applies to:

(1) a *firm* that is:

...

(e) a *Solvency II firm*;

(f) a *qualifying cryptoasset firm*.

...

...

15A.1.7 R The requirements in this chapter apply with respect to:

...

(7) any other *unregulated activities*, but only in a *prudential context*;
and

(8) *data reporting services* provided by a *consolidated tape provider*;
and

(9) activities that constitute dealing in qualifying cryptoassets as principal (article [9U]), disregarding the exclusion in article [9V] (Absence of holding out etc).

...

27 **Senior managers and certification regime: Certification regime**

...

27.8 Definitions of the FCA certification functions

...

Client-dealing function

...

27.8.19 R Table: Activities covered by the client-dealing FCA certification function

Activity	Comments
...	
(5) Acting as a ‘bidder’s representative’ in relation to <i>bidding in emissions auctions</i>
<u>Notes</u>	
<p><u>Note (1): The reference in row (3) of this table to <i>dealing</i> includes <i>issuing qualifying stablecoin</i>.</u></p>	

Note (2): The reference in row (3) of this table to *arranging (bringing about) deals in investments* includes:

- (a) *arranging deals in qualifying cryptoassets* within article [9Z] of the *Regulated Activities Order*;
- (b) *issuing qualifying stablecoin* in the *United Kingdom* where that activity would fall into (a) but for article [9Z6(4)(a)] of the *Regulated Activities Order*;
- (c) *operating a qualifying cryptoasset trading platform* where that activity would fall into (a) but for article [9Z6(4)(b)] of the *Regulated Activities Order*; and
- (d) *arranging qualifying cryptoasset staking*.

...

Annex D

Amendments to the General Provisions (GEN)

In this Annex, underlining indicates new text.

2 Interpreting the Handbook

...

2.2 Interpreting the Handbook

...

Registered persons

2.2.20A G (3) ...

(4) The exemption in article 73ZA of the *Financial Promotion Order* will only be available to a *registered person* within scope of article [14] of the [Financial Services and Markets Act 2000 (Regulated Activities and Miscellaneous Provisions) (Cryptoassets) Regulations 2025].

...

Annex E

Amendments to the Supervision manual (SUP)

In this Annex, underlining indicates new text and striking through indicates deleted text.

3 **Auditors**

3.1 **Application**

...

3.1.2 R Applicable sections (see *SUP* 3.1.1R)

...

(1) Category of firm		(2) Sections applicable to the firm	(3) Sections applicable to its auditor
...			
(12)
(13)	<u>qualifying stablecoin issuer</u>	<u><i>SUP</i> 3.1 – <i>SUP</i> 3.7, <i>SUP</i> 3.11</u>	<u><i>SUP</i> 3.1, <i>SUP</i> 3.2, <i>SUP</i> 3.8, <i>SUP</i> 3.10</u>
(14)	<u>qualifying cryptoasset custodian</u>	<u><i>SUP</i> 3.1 – <i>SUP</i> 3.7, <i>SUP</i> 3.11</u>	<u><i>SUP</i> 3.1, <i>SUP</i> 3.2, <i>SUP</i> 3.8, <i>SUP</i> 3.10</u>
...			

...

3.3 **Appointment of auditors**

...

Appointment by the appropriate regulator

3.3.7 R (1) Paragraph (2) applies to a *firm* which is not under an obligation to appoint an auditor imposed by an enactment other than the *Act*.

(2) If a *firm* fails to appoint an auditor within 28 days of a vacancy arising, the *appropriate regulator* may appoint an auditor for it on the following terms:

- (a) the auditor to be remunerated by the *firm* on the basis agreed between the auditor and *firm* or, in the absence of agreement, on a reasonable basis; and
- (b) the auditor to hold office until ~~he resigns~~ they resign or the *firm* appoints another auditor.

...

3.4 Auditors' qualifications

Purpose

3.4.1 G The *appropriate regulator* is concerned to ensure that the auditor of a *firm* has the necessary skill and experience to audit the business of the *firm* to which ~~he has~~ they have been appointed. This section sets out the *appropriate regulator's rules* and *guidance* aimed at achieving this.

Qualifications

3.4.2 R Before a *firm*, to which SUP 3.3.2R applies, appoints an auditor, it must take reasonable steps to ensure that the auditor has the required skill, resources and experience to perform ~~his~~ their functions under the *regulatory system* and that the auditor:

...

...

Disqualified auditors

...

3.4.6 G If it appears to the *appropriate regulator* that an auditor of a *firm* has failed to comply with a duty imposed on ~~him~~ them under the *Act*, it may have the power to and may disqualify ~~him~~ them under section 345 or 345A, respectively, of the *Act*. A list of *persons* who are disqualified may be found on the *FCA*'s website (www.fca.org.uk).

...

3.5 Auditors' independence

Purpose

3.5.1 G If an auditor is to carry out ~~his~~ their duties properly, ~~he needs~~ they need to be independent of the *firm* ~~he is~~ they are auditing, so that ~~he is~~ they are not subject to conflicts of interest. Many *firms* are also subject to requirements under the Companies Act 1989, or the Companies Act 2006, the Building Societies Act 1986 or the Friendly Societies Act 1992 on auditor's independence.

...

Independence

...

3.5.4 G The *appropriate regulator* will regard an auditor as independent if his their appointment or retention does not breach the ethical guidance in current issue from the auditor's recognised supervisory body on the appointment of an auditor in circumstances which could give rise to conflicts of interest.

...

3.6 Firms' cooperation with their auditors

3.6.1 R A *firm* must cooperate with its auditor in the discharge of his their duties under this chapter.

Auditor's access to accounting records

3.6.2 G In complying with *SUP 3.6.1R*, a *firm* should give a right of access at all times to the *firm*'s accounting and other records, in whatever form they are held, and *documents* relating to its business. A *firm* should allow its auditor to copy *documents* or other material on the premises of the *firm* and to remove copies or hold them elsewhere, or give him them such copies on request.

3.6.3 G Section 341 of the Act (Access to books etc.) provides that an auditor of a *firm* appointed under *SUP 3.3.2R*:

...

(2) is entitled to require from the *firm*'s officers such information and explanations as he they reasonably considers consider necessary for the performance of his their duties as auditor.

...

Access and cooperation: appointed representatives, material outsourcing, employees

...

3.6.8 G In complying with *SUP 3.6.1R*, a *firm* should take reasonable steps to ensure that all its employees cooperate with its auditor in the discharge of his their duties under this chapter.

...

3.7 Notification of matters raised by auditor

...

Notification

3.7.2 G A *firm* should consider whether it should notify the *FCA* and the *PRA* (if it is a *PRA-authorised firm*) or the *FCA* (in all other cases) under *Principle 11* if:

- (1) the *firm* expects or knows its auditor will qualify his their report on the audited annual financial statements or add an explanatory paragraph; or

...

...

3.8 Rights and duties of auditors

Purpose

3.8.1 G The auditor of a *firm* has various rights and duties to obtain information from the *firm* and both to enable and to require him them to pass information to the *appropriate regulator* in specified circumstances. This section imposes or gives *guidance* on those rights and duties.

...

Auditor's independence

3.8.5 R An auditor of a *firm* must be independent of the *firm* in performing his their duties in respect of that *firm*.

3.8.6 R An auditor of a *firm* must take reasonable steps to satisfy himself themselves that he is they are free from any conflict of interest in respect of that *firm* from which bias may reasonably be inferred. He They must take appropriate action where this is not the case.

...

Communication between the appropriate regulator, the firm and the auditor

3.8.9 G Within the legal constraints that apply, the *appropriate regulator* may pass on to an auditor any information which it considers relevant to his their function. An auditor is bound by the confidentiality provisions set out in Part XXIII of the Act (Public record, disclosure of information and cooperation) in respect of confidential information he receives they receive from the *appropriate regulator*. An auditor may not pass on such confidential information without lawful authority, for example if an exception applies under the Financial Services and Markets Act 2000 (Disclosure of Confidential Information) Regulations 2001 (SI 2001/2188) or with the consent of the *person* from whom that information was received and (if different) to whom the information relates.

Auditors' statutory duty to report

3.8.10 G ...

(2) These regulations oblige auditors to report certain matters to the *appropriate regulator*. Sections 342(3) and 343(3) of the *Act* provide that an auditor does not contravene any duty by giving information or expressing an opinion to the *appropriate regulator*, if ~~he is~~ they are acting in good faith and ~~he~~ they reasonably ~~believe~~ believe that the information or opinion is relevant to any functions of the *appropriate regulator*. These provisions continue to have effect after the end of the auditor's term of appointment.

In relation to Lloyd's, an effect of the *insurance market direction* set out at SUP 3.1.13D is that sections 342(5) and 343(5) of the *Act* (Information given by an auditor or actuary to a regulator) apply also to auditors appointed to report on the *insurance business of members*.

Termination of term of office, disqualification

3.8.11 R An auditor must notify the *appropriate regulator* without delay if ~~he~~ they:

- (1) ~~is~~ are removed from office by a *firm*; or
- (2) ~~resigns~~ resign before ~~his~~ their term of office expires; or
- (3) ~~is~~ are not re-appointed by a *firm*.

3.8.12 R If an auditor ceases to be, or is formally notified that ~~he~~ they will cease to be, the auditor of a *firm*, ~~he~~ they must notify the *appropriate regulator* without delay:

- (1) of any matter connected with ~~his~~ their so ceasing which ~~he thinks~~ they think ought to be drawn to the *appropriate regulator*'s attention; or

...

3.10 Duties of auditors: notification and report on client assets

...

Client assets report: content

3.10.4 R An auditor of a *firm* must submit a client assets report addressed to the *FCA* which:

- (1) (a) states the matters set out in SUP 3.10.5R; and
- (b) specifies the matters to which SUP 3.10.9R and SUP 3.10.9AR refer; or

(2) if the *firm* claims not to hold *client money, qualifying cryptoassets in the course of carrying on the regulated activity specified in article [9O(1)(a)] of the Regulated Activities Order, stablecoin backing assets, stablecoin backing funds* or *custody assets*, states whether anything has come to the auditor's attention that causes *him them* to believe that the *firm* held *client money, qualifying cryptoassets in the course of carrying on the regulated activity specified in article [9O(1)(a)] of the Regulated Activities Order, stablecoin backing funds, stablecoin backing assets* or *custody assets* during the period covered by the report.

3.10.5 R Client assets report

Whether in the auditor's opinion	
...	
(3)	in the case of an <i>investment management firm, personal investment firm, a UCITS firm, securities and futures firm, firm acting as trustee or depositary of an AIF, firm acting as trustee or depositary of a UK UCITS or a MIFIDPRU investment firm</i> , when a <i>subsidiary</i> of the <i>firm</i> is during the period a <i>nominee company</i> in whose name <i>custody assets</i> of the <i>firm</i> are registered during the period, that <i>nominee company</i> has maintained throughout the period systems for the custody, identification and control of <i>custody assets</i> which:
	(a) were adequate; and
	(b) included reconciliations at appropriate intervals between the records maintained (whether by the <i>firm</i> or the <i>nominee company</i>) and statements or confirmations from <i>custodians</i> or from the <i>person</i> who maintained the record of legal entitlement; and
(4)	if there has been a <i>secondary pooling event</i> during the period, the <i>firm</i> has complied with the <i>rules</i> in <i>CASS 5.6</i> and <i>CASS 7A</i> (Client money distribution), <i>CASS 11.13</i> (debt management client money distribution rules) and <i>CASS 13.11</i> (claims management client money distribution rules) in relation to that pooling event;:
(5)	<u>in the case of a qualifying stablecoin issuer, the firm was in compliance with CASS 16; and</u>
(6)	<u>in the case of a firm which is safeguarding qualifying cryptoassets or arranging qualifying cryptoasset safeguarding, the firm was in compliance with CASS 17.</u>

...

Client assets report: requirements not met or inability to form opinion

3.10.9 R If the client assets report under *SUP 3.10.4R* states that one or more of the applicable requirements described in *SUP 3.10.5 R(1)* to ~~(4) (6)~~ has or have not been met, the auditor must specify in the report each of those requirements and the respects in which it has or they have not been met.

3.10.9A R (1) Whether or not an auditor concludes that one or more of the requirements specified in *SUP 3.10.5 R(1)* to ~~(4) (6)~~ has or have been met, the auditor must ensure that the client assets report identifies each individual *rule* in respect of which a breach has been identified.

...

3 Annex SUP 3 Annex 1

Auditor's client assets report - SUP 3 Annex 1

SUP 3 Annex 1R

Auditor's client assets report Part 1 – Auditor's Opinion

Independent auditor's report on client assets to the Financial Conduct Authority in respect of [Firm name], firm reference number [number], for the period started [dd/mm/yyyy] and ended [dd/mm/yyyy]

Part 1: Auditor's Opinion on Client Assets

...

Opinion

In our opinion:

[The firm has maintained] [Except for....the firm has maintained] [Because of....the firm did not maintain] systems adequate to enable it to comply with [the custody rules,] [the collateral rules,] [the mandate rules,] [the client money rules,] [CASS 16,] [CASS 17] [and] [the debt management client money rules] throughout the period since [the last date at which a report was made] [the firm was authorised] [the firm became subject to SUP 3.11 and we, its auditor, became subject to SUP 3.10].*

[The firm was] [Except for....the firm was] [Because of....the firm was not] in compliance with ~~the~~ [the custody rules,] [the collateral rules,] [the mandate rules,] [the client money rules,] [CASS 16,] [CASS 17] [and] [the debt management client money rules] as at the period end date.*

~ / ~

The scope of the firm's permissions did not allow it to hold [stablecoin backing assets] [stablecoin backing funds] [qualifying cryptoassets in the course of carrying on the regulated activity specified in article [9O(1)(a)] of the Regulated Activities Order] [client money] [or] [custody assets].

The directors (or equivalent corporate officers) of the firm have stated that the firm did not hold [stablecoin backing assets] [stablecoin backing funds] [qualifying cryptoassets in the course of carrying on the regulated activity specified in article [9O(1)(a)] of the Regulated Activities Order] [client money] [or] [custody assets] during the period. Based on review procedures performed, nothing has come to our attention that causes us to believe that the firm held [stablecoin backing assets] [stablecoin backing funds] [qualifying cryptoassets in the course of carrying on the regulated activity specified in article [9O(1)(a)] of the Regulated Activities Order] [client money] [or] [custody assets] during the period.

...

Instructions for Part 1:

* If the auditor expresses an adverse opinion (i.e. states the firm 'did not maintain...' or 'was not in compliance...') ~~he~~ they must set out the reasons why. This can be done by reference to items in columns A to D in Part 2 of the auditor's report on client assets.

If the auditor expresses a qualified opinion (i.e. states 'that except for, the firm did maintain' or 'that except for, the firm was in compliance') ~~he~~ they must do so by reference to items in columns A to D in Part 2 of the auditor's report on client assets.

...

...

© Financial Conduct Authority 2025
12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk
All rights reserved

Pub ref: 2-008491

All our publications are available to download from www.fca.org.uk.

Request an alternative format

Please complete this [form](#) if you require this content in an alternative format.

Or call 0207 066 1000



[**Sign up**](#) for our **news and publications alerts**