

CP26/23 – Operational resilience: Critical third parties to the UK financial sector

**Consultation paper 26/23 | FCA
consultation paper 23/30**

7 December 2023

Contents

1: Overview	5
Background	7
Structure of this consultation paper	10
Overview of the proposals in this consultation paper	12
Cost benefit analysis (CBA)	14
Legal obligations	15
Implementation	15
Responses and next steps	15
2: Identifying potential critical third parties and recommending them for designation	17
Assessing whether a third party meets the statutory test for designation by HMT as a CTP	19
Materiality	20
Concentration	21
Other relevant factors	22
3: Key terms	23
4: CTP Fundamental Rules	25
Box A: Proposed critical third party Fundamental Rules	25
5: CTP Operational Risk and Resilience Requirements	26
Box B: Minimum resilience standards for CTPs in DP3/22	26
6: Information-gathering, self-assessment, testing, Skilled Person Review and information sharing	38
General evidence and information requirement	39
Self-assessment	39
Testing requirements	39
7: Notifications	43

Relevant incident	44
Phased approach to incident notifications	45
Format of incident notifications	45
Incident notification triggers and initial incident notification	45
Intermediate incident notifications	46
Final incident notification	46
Other notification requirements	47
8: Misleading use of designation status	47
Public references to a CTP's designated status	47
9: Nomination of a legal person for non-UK CTPs	49
Nomination of a legal person	49
10. Record keeping and emergency relief	49
Emergency	50
11: Regulators' statutory obligations	51
Regulators' objectives analysis	51
Statutory obligations relating to competition	53
FCA and PRA Secondary competitiveness and growth objective	54
Regulators' 'have regards' analysis	54
Bank of England additional 'have regards' analysis	59
12: Questions	61

Privacy statement

By responding to this consultation, you provide personal data to the Bank of England (the Bank, which includes the Prudential Regulation Authority (PRA)), and the Financial Conduct Authority (FCA). This may include your name, contact details (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself.

The response will be assessed to inform our work as regulators and a central bank, both in the public interest and in the exercise of our official authority. We may use your details to contact you to clarify any aspects of your response.

The consultation paper will explain if responses will be shared with other organisations. If this is the case, the other organisation will also review the responses and may also contact you to clarify aspects of your response. We will retain all responses for the period that is relevant to supporting ongoing regulatory policy developments and reviews. However, all personal data will be redacted from the responses within five years of receipt. To find out more about how we deal with your personal data, your rights, or to get in touch please visit [Privacy and the Bank of England](#). To find out more about how the FCA deals with your personal data please visit the [FCA's privacy page](#).

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure to other parties in accordance with access to information regimes including under the Freedom of Information Act 2000 or data protection legislation, or as otherwise required by law or in discharge of the Bank's or FCA's functions. Please indicate if you regard all, or some of, the information you provide as confidential. If the Bank receives a request for disclosure of this information, we will take your indication(s) into account but cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system on emails will not, of itself, be regarded as binding on us.

Responses are requested by 15 March 2024.

Consent to publication

The Bank and FCA publishes a list of respondents to its consultations, where respondents have consented to such publication.

When you respond to this consultation paper (CP), please tell us in your response if you agree to the publication of your name, or the name of the organisation you are responding on behalf of, in the PRA, Bank and FCA's feedback response to this consultation.

Please make it clear if you are responding as an individual or on behalf of an organisation.

Where your name comprises 'personal data' within the meaning of data protection law, please see the Bank and FCA's Privacy Notice above, about how your personal data will be processed.

Please note that you do not have to give your consent to the publication of your name. If you do not give consent to your name being published in the feedback response to this consultation, please make this clear with your response.

If you do not give consent, the PRA, Bank and FCA may still collect, record and store it in accordance with the information provided above.

You have the right to withdraw, amend or revoke your consent at any time. If you would like to do this, please contact the PRA using the contact details set out below.

Responses can be sent by email to: CP26_23@bankofengland.co.uk.

Alternatively, please address any comments or enquiries to:

The Recovery, Resolution and Resilience Team

Prudential Regulation Authority

20 Moorgate

London

EC2R 6DA

1: Overview

1.1 This consultation paper (CP) is issued jointly by the Prudential Regulation Authority (PRA), the Financial Conduct Authority (FCA), and the Bank of England (Bank) (collectively 'the regulators'). It sets out the proposed requirements to be established in rules and accompanying expectations for critical third parties (CTPs). For the purpose of this CP, a CTP is an entity that will be designated by HM Treasury (HMT) by a regulation made in exercise of the power in section 312L(1) of the [Financial Services and Markets Act 2000](#) (FSMA) as amended by the [Financial Services and Markets Act 2023](#) (FSMA 2023).

1.2 The key aim of the proposed requirements and expectations in this CP is to manage potential risks to the stability of, or confidence in, the UK financial system that may arise due to a failure in, or disruption to, the services that a CTP provides to one or more authorised persons, relevant service providers (collectively 'firms'), and/or financial market infrastructure entities ('FMIs') (either individually or, where more than one service is provided, taken together).

1.3 The regulators consider that the proposals in this CP would allow them to monitor and manage the risks referred to above in an effective but proportionate manner and advance their respective objectives. Crucially, the proposals in this CP will complement but not blur, eliminate, or reduce the accountability and responsibility of firms, FMIs, their boards, and senior management (including any individuals performing Senior Management Functions (SMFs)) from continuing to fulfil their existing regulatory obligations on operational resilience and third-party risk management.

1.4 The proposals would result in:

- requirements for CTPs in the Bank Rulebook, PRA Rulebook, and FCA Handbook;
- a joint Bank/PRA/FCA supervisory statement setting out the regulators' expectations of how CTPs should comply with and interpret the proposed requirements in their rules; and
- a joint Bank/PRA supervisory statement and FCA guidance on the regulators' policy and expectations on the use of skilled person reviews of CTPs as an oversight tool.

1.5 The Bank and the PRA also intend to consult on a joint statement of policy in relation to the use of their disciplinary powers over CTPs in due course, which will be aligned to their ongoing wider review of [enforcement](#). To maintain a joint approach to

the CTP oversight regime across the three regulators, the FCA intends to consult on its statement of policy on the use of disciplinary powers over CTPs around the same time.

1.6 The regulators also intend to publish a document setting out how they will carry out their oversight roles in relation to CTPs ('CTP approach document') in due course. The CTP approach document will help CTPs, firms, and FMIs understand how the regulators will oversee CTPs in practice and uphold the regulators' accountability to the public and Parliament through greater transparency.

1.7 Throughout this CP, unless otherwise stated:

- 'requirement' and related terms describe the regulators' proposed rules; and
- 'expectation' and related terms describe the regulators' proposed expectations of how CTPs should comply with and interpret the proposed requirements in the draft rules. These expectations are set out in the draft supervisory statement.

1.8 Likewise, throughout the draft supervisory statement:

- 'must' describes a proposed requirement in FSMA or the regulators' rules; and
- 'should' sets out the regulators' proposed expectations on how CTPs should comply with a proposed requirement.

1.9 To ensure a clear and consistent understanding of the proposals and the terminology used, this CP should be read alongside the draft rules and the draft supervisory statement.

Scope

1.10 The CP is primarily relevant to CTPs. At the time of publication of this CP, HMT had not designated any third parties as CTPs. Chapter 2 of this CP seeks to provide clarity on the regulators' approach and criteria to identifying potential CTPs and recommending them for designation to HMT (without prejudice to any future designation decisions by HMT).

1.11 The CP is also relevant to firms and FMIs. The proposals in this CP would not impose additional requirements on firms and FMIs but seek to complement their existing obligations on operational resilience and third-party risk management.

1.12 Firms and FMIs are reminded that a CTP's designated status will not necessarily mean that it is inherently more resilient, safer, or more suitable to provide a given service to a given firm or FMI than non-designated third parties providing the same or similar services. As set out in Chapter 2, the regulators intend to recommend third parties for designation as CTPs based on their assessment of the potential impact that a failure in, or disruption to, these third parties' services could have on the stability of,

or confidence in, the UK financial system. Nevertheless, firms and FMIs will remain accountable and responsible for assessing the materiality and risks for each of their outsourcing and third party arrangements and performing appropriate and proportionate due diligence on potential third parties.

Focus on CTPs' services to firms and FMIs

1.13 The proposals in this CP would apply only to CTPs' services to firms and FMIs.

1.14 The regulators propose to apply the CTP Fundamental Rules in section 4 to all of the services that a CTP provides to firms and FMIs. The regulators propose that other (more granular) requirements will only apply to a CTP's material services. For instance, the Operational Risk and Resilience Requirements in section 5, the scenario testing requirements in section 6 and the incident notification requirements in section 7. As explained in the regulators' draft rules and joint draft supervisory statement, material services encompass those services whose failure or disruption could threaten the stability of, or confidence in, the UK financial system. They are also the services that HMT must have regard to when designating a CTP.

1.15 The proposed requirements in this CP would apply to services provided to firms and FMIs regulated by the Bank, PRA, and/or FCA (wherever carried out). The proposals are therefore agnostic as to the location of a CTP. There is no requirement for a CTP to set up a UK establishment (e.g. a subsidiary) where one does not already exist. This proposed approach recognises that CTPs may provide services from multiple jurisdictions (which can help improve the efficiency and resilience of these services). Likewise, the firms and FMIs that receive services from CTPs may operate in multiple jurisdictions. This proposed approach could also reduce compliance costs for CTPs, firms and FMIs compared to an approach that required CTPs to localise entities, infrastructure, personnel, or services in the UK.

1.16 To ensure the efficient operation of the proposed oversight regime for CTPs, certain proposals in this CP seek to ensure that there is a central point of contact for the regulators at every CTP and, for those CTPs whose head office is not in the UK, a legal person to perform certain functions on their behalf such as receiving statutory notices issued by the regulators under FSMA.

Background

The Financial Policy Committee's focus on CTPs

1.17 The Bank's Financial Policy Committee (FPC) has been monitoring the potential systemic risks posed by CTPs for several years. In the [June 2017 Financial Stability Report](#) (FSR), the FPC 'requested annual updates from the financial authorities on the

cyber resilience of firms that are outside the regulatory perimeter, but which are important for the UK financial sector’.

1.18 In the [November 2018 FSR](#), the FPC began closely monitoring cloud service providers (CSPs) in particular after noting that, due to high concentration in the market for cloud services, ‘disruption at one provider, for example due to cyber-attack, could interfere with the provision of vital services by several firms’.

1.19 The [FPC’s Q2 2021 Financial Policy Summary and Record](#) noted that, ‘since the start of 2020, financial institutions have accelerated plans to scale up their reliance on CSPs and in future place vital services on the cloud’. It concluded, that ‘the increasing reliance on a small number of CSPs and other CTPs for vital services could increase financial stability risks in the absence of greater direct regulatory oversight of the resilience of the services they provide’.

1.20 The FPC restated these views in the Q3 2021 [Financial Policy Summary and Record](#) and [Q1 2022 Financial Policy Summary and Record](#).

Legislative changes

1.21 [FSMA 2023](#) granted HMT and the regulators powers in relation to CTPs, which provide the statutory basis for the proposals in this CP. In particular, it gave HMT the power to designate certain third parties as CTPs, and gave the regulators powers to:

- make rules imposing duties on CTPs in connection with their provision of services to firms and FMIs (s312M of FSMA) (‘rulemaking powers’);
- direct a CTP in writing to (a) do anything or (b) refrain from doing anything specified in the direction (s312N FSMA) (‘powers of direction’);
- gather information from a CTP and persons connected¹ to a CTP, appoint or direct the appointment of skilled persons, and carry out investigations (s312P FSMA) (‘information-gathering and investigatory powers’); and
- take enforcement action against a CTP in certain circumstances (s312Q and s312R FSMA) (‘disciplinary powers’).

1.22 The regulators’ new statutory powers seek to enable them to intervene to raise the resilience of the services that CTPs provide to firms and FMIs, thereby reducing the risk of systemic disruption to the financial sector.

¹ Persons connected to a CTP has been defined in section 312P(10) of FSMA and the regulators’ draft rules.

Discussion paper (DP) 3/22 – Operational Resilience: Critical Third Parties to the UK Financial Sector

1.23 DP3/22 – Operational resilience: Critical third parties to the UK financial sector, which was issued jointly by the regulators, sought views on potential policy measures to manage the systemic risks posed by certain third parties to the UK financial sector, and how the services they provide could be made more resilient in order to advance the regulators' objectives.

1.24 DP3/22 recognised the potential benefits that services provided by third parties can bring to firms and FMIs and underscored the regulators' support for the safe and sustainable use of these services. However, it also noted that the failure of certain third parties, or severe disruption to the material services that they provide to firms and FMIs, could pose risks to the financial stability of the UK, which provided a case for regulatory intervention.

1.25 The regulators received 58 responses to DP3/22 from a range of stakeholders, including financial institutions, third parties, and industry bodies. The regulators also received views from their respective independent Practitioner Panels.

1.26 The key themes in responses to DP3/22 were:

- **Broad support for regulatory intervention:** Most of the respondents to the DP agreed that firms' and FMIs' increasing reliance on certain third parties could pose systemic risk to the regulators' objectives and supported the need for greater direct regulatory oversight. There was strong support for the introduction of a framework for CTPs that is principles-based, proportionate, and outcomes-focused along the lines proposed in the DP. However, several respondents noted that any additional measures for CTPs should be proportionate and not unduly restrict the ability of firms and FMIs to choose third party service providers.
- **International co-ordination and cooperation:** Respondents consistently and strongly encouraged greater international regulatory and supervisory coordination and co-operation in the area of CTPs. In particular, respondents encouraged coordination with jurisdictions or regions that have, or are in the process of developing, similar regimes for CTPs.
- **Interaction with the existing regulatory framework for firms and FMIs:** Respondents urged the regulators not to impose additional requirements on firms and FMIs, and to be clear about the respective roles and responsibilities of firms and FMIs on the one hand, and CTPs on the other.
- **Minimum Resilience Standards:** Respondents supported the idea of a set of minimum resilience standards for the services that CTPs provide to firms and

FMI. Respondents encouraged the regulators to draw inspiration from existing global principles, such as the Basel Committee on Banking Supervision's (BCBS) [Principles for operational resilience](#) and [Revised Principles for the Sound Management of Operational Risk](#) (PSMORs) when developing these standards. There were also extensive comments on the detail of certain individual potential standards, such as those relating to the identification and mapping of CTP's material services, or the development of financial sector continuity playbooks.

- **Information Sharing:** Several respondents encouraged the regulators to share relevant information about the resilience of CTPs' services obtained through their potential future oversight with firms and FMIs to inform their operational resilience and third-party risk management. However, respondents cautioned that, when sharing this information, regulators would need to consider issues such as confidentiality, market sensitivity and information security.
- **Testing:** Respondents encouraged the regulators to adopt an agile, proportionate approach to testing the resilience of CTP's services, and to use a range of testing tools. Some respondents encouraged the regulators to take into account the results of testing performed by CTPs internally, and by or on behalf of other regulators.
- **Cross-sectoral coordination and cooperation:** Respondents encouraged the regulators to consider how the proposed CTP regime would interact with UK cross-sectoral legislation in areas such as cyber-security and data protection, and how they would coordinate with relevant, non-financial UK authorities.

1.27 Throughout this CP, the regulators have explained how and where responses to DP3/22 have informed the development of their proposals.

Structure of this consultation paper

1.28 This CP is structured into the following chapters:

- **Identifying potential CTPs and recommending them for designation (Chapter 2):** [HMT will designate](#) each CTP based on the services it provides to firms and FMIs, and has stated that 'designation will generally follow a recommendation from the regulators'. This chapter sets out the regulators' evolving thinking on how they may identify potential CTPs to recommend to HMT for designation. It includes the criteria the regulators are considering using, which is based upon the statutory test for designation in s312L FSMA that HMT will apply when it decides whether to designate a third party as a CTP, and the sources of data and information that the regulators intend to use to inform this assessment.

-
- **Key terms (Chapter 3):** This chapter sets out the key terms that the regulators propose to use in their rules and joint supervisory statement.
 - **CTP Fundamental rules (Chapter 4):** This chapter contains a set of proposed, high-level CTP Fundamental Rules that CTPs would be required to comply with in respect of all the services they provide to firms and FMIs.
 - **CTP operational risk and resilience requirements (Chapter 5):** This chapter sets out eight proposed Operational Risk and Resilience requirements, which CTPs would be required to comply with in respect of their material services to firms and FMIs.
 - **Information-gathering and testing, self-assessment and information sharing (Chapter 6):** This chapter includes proposed information-gathering and testing requirements and expectations for CTPs, including:
 - the submission of an annual self-assessment to the regulators;
 - requirements on CTPs to:
 - regularly test their ability to continue providing material services in severe but plausible scenarios (referred to as ‘scenario testing’); and
 - annually test their financial sector incident management playbook jointly with an appropriately representative sample of the firms and FMIs they provide services to;
 - requirements relating to skilled person reviews of CTPs; and
 - requirements on CTPs to share certain information with the firms and FMIs they provides services to.
 - **Notifications (Chapter 7):** This chapters sets out proposed requirements for CTPs to notify certain incidents to the regulators, and to the firms and FMIs to which they provide the impacted services. The regulators propose a phased approach to incident notifications by CTP, and have set out the information that CTPs would be required to include in each phase.
 - **Referrals to oversight by the regulators (Chapter 8);** This chapter contains proposed requirements that a CTP, and persons acting on their behalf, would have to abide by when publicly referring to their designated status, or to the fact that they are overseen by the regulators.
 - **HMT designation and nomination of a legal person in the UK and emergency relief (Chapter 9):** The chapter includes proposed requirements for CTPs without a UK head office to nominate a legal person to perform certain functions on their behalf. It also includes proposals around record keeping and Bank proposals that are intended to provide relief to a CTP in an emergency circumstances.

Overview of the proposals in this consultation paper

Format of the regulators' draft rules

1.29 Each regulator has a statutory power to make rules for CTPs. However, the regulators also have a statutory duty to coordinate the exercise of their oversight functions over CTPs (s312U FSMA), including their respective rulemaking powers.

1.30 As a result, while the regulators have different statutory objectives, the proposed requirements for CTPs in this CP are set out in three identical but separate rule instruments issued by each of the regulators. The three rule instruments are identical in effect and substance and should be interpreted accordingly. Any differences reflect non-substantive differences in the drafting style of the regulators and the format of their respective handbooks, rulebooks etc.

1.31 The regulators propose to apply the three draft rule instruments to all CTPs designated by HMT, regardless of the specific firms and FMIs to whom the CTP provides services. Consequently, a CTP should be able to pick up any of the three draft rule instruments in this CP and understand all the proposed requirements it would be subject to. References to the 'draft rules' throughout this CP, and the 'regulators' rules' in the draft supervisory statement should be interpreted as encompassing all three draft rule instruments.

1.32 To further facilitate CTPs' understanding of, and future compliance with the regulators' respective draft rules, the regulators propose that the draft joint Bank/PRA/FCA supervisory statement should be a key source of guidance for CTPs on how to approach, comply with, and interpret the regulators' proposed requirements.

1.33 At the start of each chapter and, where appropriate, other sections of this CP and the draft supervisory statement, the regulators have highlighted where the relevant proposed requirements are located in each of their respective draft rule instruments.

1.34 As required by s312V FSMA, HMT will lay before Parliament the regulators' memorandum of understanding (MoU) setting out how they intend to coordinate the exercise of their respective functions in due course. As noted above, the regulators also plan to issue a CTP approach document. The MoU and approach document will provide further details on how the regulators will coordinate their engagement with and oversight of CTPs in practice.

Interaction with the requirements for firms and FMIs

1.35 The proposals in this CP build on and complement the [operational resilience framework for firms](#) and [FMIs](#). For instance, the proposed requirements and expectations for CTPs on mapping and scenario testing were adapted from the

equivalent requirements for firms and FMIs. Moreover, like the operational resilience framework for firms and FMIs, the oversight regime for CTPs assumes that disruption will occur and seeks to ensure that CTPs prevent, adapt to, respond to, recover from, and learn from disruption (in collaboration with the firms and FMIs they provide services to where appropriate).

1.36 As noted above, the proposals in this CP do not blur, eliminate or reduce the accountability and responsibility of firms, FMIs, their boards, and senior management (including individuals performing SMFs) for their regulatory obligations on operational resilience, and outsourcing and third party risk management.

Interaction with global standards and similar non-UK regimes

1.37 The proposals in this CP draw inspiration from relevant global standards. In particular, the:

- FSB:
 - [Cyber Lexicon](#);
 - [Final report on enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities](#) (FSB TPR toolkit);
 - [Effective Practices for Cyber Incident Response and Recovery](#); and
 - [Recommendations to Achieve Greater Convergence in Cyber Incident Reporting](#) (FSB CIR Recommendations);
- Basel Committee on Banking Supervision (BCBS):
 - [Principles for operational resilience](#);
 - [Revised PSMORs](#); and
 - [High-level principles for business continuity](#); and
- Committee on Payments and Market Infrastructures-International Organization of Securities Commissions (CPMI-IOSCO):
 - [Principles for financial market infrastructures](#) (PFMIs). In particular, Annex F: ‘Oversight expectations applicable to critical service providers’; and
 - [PFMIs: Assessment methodology for the oversight expectations applicable to critical service providers](#).

1.38 The proposed oversight regime for CTPs has also been designed to be as interoperable as reasonably practicable with similar existing and future regimes, such as the EU’s [Digital Operational Resilience Act](#) (DORA) and the US’s [Bank Service Company Act](#). To promote regulatory and supervisory interoperability with these regimes, the regulators propose to:

- ask CTPs for information provided to the regulators responsible for these regimes and take it into account in their oversight; and
- accept incident notifications or reports submitted by CTPs to firms, FMIs, and/or the authorities responsible for these regimes, as long as they include the information the regulators propose to require CTPs to provide;
- explore ways to strengthen cooperation in the area of CTPs with the regulators responsible for these regimes through existing or, if necessary, new cooperation arrangements.

Cost benefit analysis (CBA)

1.39 The regulators have a statutory duty to consult when introducing new rules (ss 138I and 138J FSMA). Specifically, these sections require the FCA and the PRA to publish a CBA alongside any proposed rules, defined as an analysis of the costs, together with an analysis of the benefits that would arise if the proposed rules were made and an estimate of those costs and of those benefits, where reasonably practicable to do so.

1.40 The same requirement applies to the Bank as part of rulemaking powers set out under FSMA 2000 Schedule 17A, as amended by the FSMA 2023.

Summary of benefits and costs

1.41 The cost benefit analysis assesses the one-off and ongoing (annual) costs and benefits arising from the proposed framework. Based on the analysis of the costs and benefits of the proposals that are set out below, we expect that the proposals would bring net benefits to the UK financial sector. The full cost benefit analysis is set out in the Appendices.

1.42 The potential costs include compliance costs to CTPs directly arising from the proposals, reflecting the incremental changes that CTPs would not have undertaken in the absence of the regulation. Regulators expect there will be one-off costs to CTPs to familiarise themselves with the regime, assess their current practices against new requirements and set up processes to comply with these requirements. There would also be ongoing annual costs to CTPs to comply with the requirements. We estimate one-off and annual ongoing compliance costs of approximately £660,000-£930,000 (one-off) and £500,000 (annual on-going) respectively per CTP. We estimate total one-off and annual ongoing costs of £13-19m and c.£10m respectively, based on a population 20 CTPs as set out in HMT's Impact Assessment (the total number of CTPs that HMT will designate may ultimately vary). In addition, CTPs could incur costs for skilled persons reviews, under Sections 166 and 166A of FSMA if the regulators request a review.

1.43 The benefits would include a reduction in the likelihood of disruption at CTPs negatively impacting financial stability through improved operational resilience at CTPs, and an improved ability for the financial sector to work collaboratively with CTPs to manage the risks posed by these disruptions. Regulators have concluded that the proposals are likely to bring net benefits to the financial sector due to the important role that critical third parties are likely to play in affecting the long-term system-wide resilience of the financial sector.

Legal obligations

1.44 In carrying out policymaking functions the regulators are required to comply with several statutory obligations. Chapter 11 explains how the regulators have had regard to the obligations applicable to the regulators' policy development process, including an explanation of how this is reflected in the proposals.

Implementation

1.45 The statutory obligations of a CTP under FSMA would apply from the point it is designated by HMT. The regulators propose that the proposed requirements in their draft rules and the expectations in their joint supervisory statement would also apply from the point of designation.

1.46 Certain proposed requirements in this CP would involve the submission of certain information to the regulators on an annual basis, and the performance of certain tests by CTPs on a regular or annual basis. To ensure that CTPs have appropriate time in practice to prepare the first iteration of these submissions to the regulators, and perform the first round of mandatory testing, the regulators propose to require CTPs to:

- submit their first self-assessment to the regulators (see paragraph 6.8) within three months of designation and annually thereafter; and
- complete their first:
 - map of the resources including the assets and technology used to deliver, support, and maintain each material service it provides (see paragraphs 5.27-5.30); and
 - version of their financial sector incident management playbook (and first round of testing of the playbook) (see paragraphs 5.36-5.39 and 6.12-6.13), within the first twelve months following their designation, and annually thereafter.

Responses and next steps

1.47 This consultation closes on Friday 15 March 2024. The regulators invite feedback on the proposals set out in this consultation. Please address any comments or

enquiries to CP26_23@bankofengland.co.uk. Please indicate in your response if you believe any of the proposals in this consultation paper are likely to impact persons who share protected characteristics under the Equality Act 2010, and if so, please explain which groups and what the impact on such groups might be.

1.48 The PRA and the Bank intend to publish a further consultation paper relating to CTPs containing a draft statement of policy on their approach to the use of disciplinary powers. This will be published in due course ahead of the final policy statement that will follow this CP and contain the final rules and expectations for CTPs. To maintain a joint approach to the regime, the FCA plans to consult on their statement of policy on the use of disciplinary powers over CTPs around the same time.

1.49 As noted above, the regulators also intend to publish a 'CTP approach document' setting out how they will carry out their oversight roles in relation to CTPs) in due course.

2: Identifying potential critical third parties and recommending them for designation

2.1 Under s312L FSMA, HMT may designate a third party that provides services to one or more authorised persons, relevant service providers (collectively ‘firms’), and/or financial market infrastructure entities (‘FMIIs’)² as a CTP. HMT may only exercise this power if, in its opinion, a failure in or disruption to the provision of the services that the third party provides to firms and FMIIs (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system.

2.2 Among other conditions, under s312L HMT must consult each of the regulators before designating a third party as a CTP. In practice, this will generally involve the regulators proactively recommending to HMT that it should exercise its power to designate a third party as a CTP based on their analysis of relevant data and information.

2.3 HMT has not yet designated any third parties as CTPs. To help clarify the scope of application of this CP, this chapter sets out the regulators’ evolving thinking on how they may identify potential CTPs to recommend to HMT for designation (without prejudice to any future designation decisions by HMT). It includes the criteria the regulators intend to consider when assessing whether a third party meets the statutory test for designation in s312L FSMA, and sources of data and information they would use to support this.

Intended scope of the CTP regime

2.4 The statutory test in s312L FSMA for HMT to designate a CTP requires that the failure in or disruption to the relevant third party service provider’s services would pose a risk to the stability of, or confidence in, the UK financial system (s312L(2) FSMA). Before designating a third party service provider as a CTP, HMT must have regard to:

- the materiality of the services that the third party provides to firms and FMIIs to the delivery of essential activities, services, or operations; and

² As defined in s312L(8) of FSMA.

- the number and type of firms and FMIs to which the person provides services.

2.5 The regulators' approach to identifying potential CTPs will seek to identify third parties that meet the statutory test. CTPs are therefore expected to account for a very small number and percentage of those third parties providing services to firms and FMIs. This is in line with the original intent of the CTP regime ([as articulated by the FPC](#)) and the regulators' early thinking on their potential approach to designation ([as set out in DP3/22](#)). Industry responses to the DP overwhelmingly supported limiting the scope of the regime to systemically important third parties.

2.6 As noted in chapter 1, once designated, CTPs will be subject to the proposed requirements and expectations in this CP and be overseen by the regulators in respect of their services to firms and FMIs. The regulators propose to apply their most granular proposed requirements and expectations only to CTP's material services to firms and FMIs.

Sources of data and information

2.6 The regulators intend to develop a new policy for outsourcing and third-party (OATP) data collection and expect to [consult on this in 2024](#). The regulators expect that, over time, firm/FMI data will become the main source of data to support the identification of potential CTPs. Over the past few years, the regulators have undertaken ad-hoc data collections relating to firms' and FMIs' OATP arrangements. Data collected in this way will continue to inform the regulators' recommendations for designation until the proposed OATP register is operational.

2.7 The regulators may also take into account or cross-refer to data and information from:

- 'Material outsourcing Notifications' from firms to the:
 - PRA under Rule 2.3(1)(e) of the [Notifications](#) Part of the PRA Rulebook; and
 - FCA under the Senior Management Arrangements, Systems and Controls (SYSC) sourcebook and Supervision Manual (SUP) in the FCA Handbook.³
- Non-objection/ approval applications to the Bank by FMIs under:
 - Article 35(1) of UK [European Market Infrastructure Regulation](#) for Central Clearing Counterparties;
 - Article 19(1) of [UK CSDR for Central Securities Depositories](#); and

³ In particular, [SYSC 8.1.12G](#) and [SYSC 13.9.2G](#); and paragraph SUP 15.3.8G(1)(e).

- paragraph 5.10 of the **Outsourcing and third party risk management Supervisory Statement: recognised payment system operators and specified service providers**;
- other regulatory returns and documents obtained through supervisory engagement with firms and FMIs (eg firms' and FMIs operational resilience maps and self-assessments);
- **CBEST** and **FPC Cyber Stress Tests**;
- skilled person reviews;
- thematic reviews;
- other relevant supervisory engagement with firms and FMIs;
- non-UK regulators (eg obtained via firm and FMI supervisory colleges, and other current and potential future cooperation arrangements);
- international standard-setting bodies (SSBs) and organisations;
- UK non-financial authorities (eg the **Information Commissioner's Office (ICO)**); and
- publicly available information.

2.8 The regulators may also approach third parties they are considering recommending for designation as CTPs, which may provide these third parties with the opportunity to make available additional data and information to the regulators on a voluntary basis.

2.9 The regulators' horizon scanning may also enable them to identify and monitor third parties that may not meet the criteria for designation as a CTP at a given time but could do so in the future. For instance, third parties whose services are being adopted by firms and FMIs and whose materiality is increasing rapidly, but which the regulators do not yet deem capable to pose risks to the stability of, or confidence in, the UK financial system if disrupted.

Assessing whether a third party meets the statutory test for designation by HMT as a CTP

2.10 Section 312L(3) of FSMA requires HMT to 'have regard to the following factors when forming' that opinion on whether a third party meets the statutory test for designation as a CTP described above:

- 'the materiality of the services which the third party provides to firms and FMIs to the delivery... of essential activities, services or operations';

-
- ‘the number and type of firms and FMIs to which the third party provides services’.⁴

2.11 The regulators intend to consider these factors as part of their assessment of whether to recommend a third party to HMT for designation as a CTP. The regulators also intend to consider any other factors that are relevant to identifying whether a failure in, or disruption to, the services that a third party provides to firms and FMIs could threaten the stability of, or confidence in, the UK financial system.

2.12 The regulators therefore propose to identify potential CTPs for recommendation to HMT by assessing third parties against the following three criteria:

- materiality of the services which the third party provides to firms and FMIs;
- concentration of the services which the third party provides to firms and FMIs; and
- other drivers of potential systemic impact.

Materiality

2.13 As part of their ongoing development of a methodology for assessing the ‘materiality’ of a third party’s services, the regulators propose to build on existing regulatory publications that define systemic risk (and specific variants thereof, such as systemic cyber risk), including the:

- Bank’s **Financial Stability Strategy**;
- Bank’s 2017 **Financial Stability Report**, which discusses the nature of systemic cyber risk; and
- tools for identifying ‘systemic third-party dependencies’ in the [Financial Stability Board (FSB) **Final report on enhancing third-party risk management and oversight – a toolkit for financial institutions and financial authorities** (FSB TPR Toolkit).]

2.14 When assessing the materiality of a third party’s services, the regulators will also have regard to whether firms and FMIs have reported in the outsourcing and third party register that a third party supports their delivery of ‘Important Business Services’ as defined under the regulators’ respective operational resilience policies.⁵ However, the fact that a firm or FMI does or does not identify a third party as supporting the delivery

⁴ **The Financial Services & Markets Act, s312L.**

⁵ PRA, FCA and Bank DP1/18 – **Operational Resilience: Impact tolerances for important business services**, July 2018.

of an important business service would not override or substitute the regulators' own assessment of whether a third party meets the 'materiality' criterion.

2.15 s312L FSMA requires HMT to consider whether the failure in or disruption to the provision of a third party's services to firms and FMIs 'either individually or, where more than one service is provided, taken together could threaten the stability of, or confidence in, the UK financial system'. Therefore, the regulators propose to treat multiple distinct services provided by the same service provider to firms and FMIs as material in aggregate if they consider that their combined disruption or failure could threaten the stability of, or confidence in, the UK financial system. Where multiple third parties provide the same type of service to firms and FMIs this would be captured under the concentration criterion set out above.

Concentration

2.16 In its Q2 2021 [Financial Policy Summary and Record](#), the FPC identified growing concentration in the provision of third party services to firms and FMIs as a key driver of risk to the UK financial system, and hence a key motivation for the CTP regime. The Q3 2021 Financial Policy Summary and Record stated that 'additional policy measures, some requiring legislative change, are likely to be needed to mitigate the financial stability risks stemming from concentration in the provision of some third-party services'.

2.17 As noted in the FSB TPR toolkit, concentration in the provision of third-party services to firms or FMIs does not automatically pose systemic risks, nor is it inherently or invariably problematic. Concentration can reflect the quality, including the resilience, of a third party's services. However, in line with the comments of the FPC, the greater the share of the financial sector relying on a third party, the greater the risk to the UK financial system in the event of a failure in, or disruption to, the services that the third party provides.

2.18 As set out above, when deciding whether to designate a third party, HMT must consider the 'number and type' of firms and FMIs to whom the third party provides services. The regulators will carry out their analysis accordingly when assessing concentration for the purposes of identifying potential CTPs. This analysis will consider the use of a third party's services by firms and FMIs across the financial system as a whole and, where relevant, within individual financial markets. The regulators will also take into account the extent to which any of those firms and FMIs are systemically important individually or collectively.

Other relevant factors

2.19 When identifying potential CTPs, the regulators propose to take into account all relevant factors that affect whether a failure in, or disruption to, a third party's services to firms and FMIs could threaten the stability of, or confidence in, the UK financial system. Where data alone is insufficient to support assessment of these factors, the regulators will use judgement.

2.20 One potentially relevant factor is the substitutability of a third party's services to firms and FMIs (in particular, material services), which may arise due to:

- the lack of viable alternative providers for one or more services; or
- the potential difficulties (including risks) that firms and FMIs may face when migrating services, in particular material services, in a timely manner from one third party to another or (if applicable) back in-house.

2.21 Another potentially relevant factor is whether the third party has direct access to firms' and FMIs' people, processes, technology, facilities, data, and information (the 'resources') that support the delivery of important business services. Such access may have the potential to increase the systemic risk of any disruption or failure and hence the likelihood of designation.

Entities already subject to oversight, regulation, or supervision by the regulators

2.22 Some firms and FMIs that are already subject to regulation and supervision/oversight by one or more of the regulators may objectively meet the criteria for designation as a CTP in respect of the services they provide to other firms and FMIs. The regulators are unlikely to recommend these firms and FMIs for designation as CTPs if the relevant services that they provide to other firms and FMIs are subject to a level of regulation and oversight that delivers at least equivalent outcomes to their proposed oversight regime. Where firms and FMIs services are not subject to an appropriate level of regulation and supervision/oversight, the regulators will recommend to HMT that it designates this firm or FMI as a CTP.

2.23 The regulators are also unlikely to recommend certain third parties in other sectors (e.g. public telecommunications providers, energy suppliers) for designation if the regulators are satisfied that the services that these third parties provide to firms and FMIs are subject to a level of regulation and oversight that delivers at least equivalent outcomes to the proposed regime.

Communication with CTPs about their designation and material services (including periodic reviews)

2.24 When recommending to HMT that it designates a third party as a CTP, the regulators propose to indicate to HMT which of the third party's services to firms and FMI's they have identified as material. Potential CTPs would be able to discuss these services with HMT and the regulators during the period for making representations about their proposed designation (see s312L(4)(b) FSMA).

2.25 The regulators propose to define 'material services' in their rules as 'services provided by a CTP to one or more firms a failure in, or disruption to, the provision of which (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system.'

2.26 If HMT decides to designate a third party as a CTP, it will privately communicate its decision to the CTP prior to publishing its designation order. This communication will include an initial list of the services that are considered material at the point of designation.

2.27 The regulators will periodically review whether a CTP continues to meet the criteria for designation and update HMT accordingly. Following each of these periodic reviews, the regulators will

- recommend to HM Treasury that it removes the designation of any CTP which they consider no longer meets the statutory test for designation; and
- for those CTPs who continue to meet the criteria for legislation, flag whether the review has highlighted any potential changes to their list of material services. For instance, potential new material services, or formerly material services which may potentially no longer be material. The regulators will use this analysis to facilitate a dialogue with CTPs about possible changes to their list of material services.

3: Key terms

3.1 The regulators propose to define key terms in their draft rules and supervisory statement to ensure a clear and consistent understanding. The proposed definitions are in:

- the Glossary in the FCA Handbook;

- the 'Applications and Definitions' and 'Interpretative Provisions' chapters in the Critical Third Parties Parts of the PRA and Bank Rulebooks; and
- Chapter 2 of the draft supervisory statement.

3.2 The majority of the proposed key terms in the SS stem from:

- FSMA (as amended by FSMA 2023);
- the existing operational resilience framework for firms and FMIs; and
- the FSB [Cyber Lexicon](#) and FSB Third-Party Risk Toolkit.

3.3 The regulators propose to introduce new key terms only where they consider it to be helpful or necessary. For instance, when introducing a new concept, such as 'financial sector incident management playbook'.

4: CTP Fundamental Rules

4.1 The regulators propose to introduce a set of six Fundamental Rules that CTPs would be required to comply with in respect of all the services that they provide to firms and FMIs (wherever carried out). The proposed rules are set out in:

- Critical Third Parties Fundamental Rules chapter 3 of the Critical Third Parties (CTPS) sourcebook in the FCA Handbook;
- the Critical Third Parties Fundamental Rules chapter in the draft Critical Third Parties Parts of the PRA and Bank Rulebooks; and
- Chapter 4 of the draft Supervisory Statement sets out of the regulators' expectations of how CTPs should approach the CTP Fundamental Rules.

4.2 The proposed CTP Fundamental Rules, which are similar but less extensive than the [PRA Fundamental Rules](#) and [FCA Principles for Businesses](#) are high level rules that would collectively act as an expression of the regulators' objective of managing risks to the stability of, or confidence in, the UK financial system posed by CTPs. The proposed rules would provide a general statement of a CTP's fundamental obligations under the oversight regime and would apply to all services provided by a CTP to firms and FMIs, not only material services.

Box A: Proposed critical third party Fundamental Rules

CTP Fundamental Rule 1: A CTP must conduct its business with integrity.

CTP Fundamental Rule 2: A CTP must conduct its business with due skill, care and diligence.

CTP Fundamental Rule 3: A CTP must act in a prudent manner.

CTP Fundamental Rule 4: A CTP must have effective risk strategies and risk management systems.

CTP Fundamental Rule 5: A CTP must organise and control its affairs responsibly and effectively.

CTP Fundamental Rule 6: A CTP must deal with the regulators in an open and co-operative way, and disclose to the regulators appropriately anything relating to the CTP of which they would reasonably expect notice.

5: CTP Operational Risk and Resilience Requirements

5.1 The regulators propose to introduce eight Operational Risk and Resilience Requirements that CTPs would be required to comply with in respect of their material services. The proposed Operational Risk and Resilience Requirements are in:

- Chapter 4 of the Critical Third Parties sourcebook in the FCA Handbook; and
- the ‘Critical Third Party Operational Risk and Resilience Requirements’ in chapter 4 in the draft Critical Third Parties Parts of the PRA and Bank Rulebooks.

Background

5.2 In Chapter 5 of DP3/22, the regulators set out their initial thoughts on a potential set of ‘Minimum Resilience Standards for CTPs’ (‘standards’) that would apply to their services to firms and FMIs (see Box [B]).

Box B: Minimum resilience standards for CTPs in DP3/22

1: Identification	The CTP has identified and documented all services that it provides to firms and FMIs, which, if disrupted, could have a systemic impact on the supervisory authorities’ objectives (material services).
2: Mapping	The CTP has identified and documented the people processes, technology, facilities, and information (collectively the resources) required for delivering its material services to firms and FMIs, including key nth parties and other key parts of its supply chain.

3: Risk management	The CTP has identified risks to its material services across its supply chain, and implemented appropriate controls.
4: Testing	<p>The CTP regularly tests the resilience of its material services by:</p> <ul style="list-style-type: none"> • participating in tests and sector-wide exercises convened by the supervisory authorities; and • performing its own tests.
5: Engagement with the supervisory authorities	The CTP proactively and promptly discloses to the supervisory authorities any information of which they would reasonably expect notice. In particular, information relating to incidents or threats that could have a systemic impact on the supervisory authorities' objectives.
6: Financial sector continuity playbook	The CTP has developed and, to the extent appropriate, tested specific measures to address potential systemic risks to the supervisory authorities' objectives that could arise from its failure, or a severe but plausible disruption to its material services to firms and FMIs. The CTP has documented these measures in a 'Financial sector continuity playbook', which it regularly updates and submits to the supervisory authorities.
7 Post-incident communication	The CTP has developed a tailored communication plan to engage with firms, FMIs, the supervisory authorities, and other relevant stakeholders in the event of its failure, or a severe disruption to its material services. The communication plan should include proposed steps to manage the risk of a loss of confidence in

	<p>the financial system linked to the CTP's failure or disruption. For instance, by including appropriate information about any measures that the CTP would take to recover or restore the material services, and the estimated timeframes for doing so.</p>
8 Learning and evolving	<p>The CTP learns from any:</p> <ul style="list-style-type: none"> • severe disruption it experiences; • known severe disruption at other relevant third parties; • disruption at the firms and FMIs to which it provides services; and • resilience tests and sector exercises that it performs or participates in. The CTP applies lessons learnt to the remediation of vulnerabilities, updates to existing services, and the development new services. <p>The CTP regularly shares these lessons with firms and FMIs and the supervisory authorities.</p>

5.3 The potential minimum resilience standards set out in DP3/22 generated extensive responses. There was support for the idea of clear, principles-based, outcomes-focused requirements for CTPs. However, respondents urged the regulators to avoid excessively granular or prescriptive requirements. Most of the responses focused on the detail of individual standards. In particular, respondents:

- noted that the 'Identification' standard could be unworkable for some potential CTPs as:
 - the materiality of their services depends on how their customers use them; and
 - they do not know what firms and FMIs use their services for;
- wanted greater clarity on what the standard on 'Engagement with the Supervisory Authorities' may involve, in particular, whether it may include incident notification requirements for CTPs;

- supported the idea of a ‘financial sector continuity playbook’ but:
 - cautioned that requiring CTPs to implement business continuity plans, contingency plans, and other measures specifically for their firm and FMI customers could cause them to segregate their services to these customers from those services that they provide to other sectors, which could have adverse unintended consequences including diminished resilience of the relevant services, and higher costs for firms and FMIs;
 - suggested that the financial sector continuity playbook should focus on coordination and communication between CTPs, their firm, and FMI customers and the regulators during an incident; and
 - recommended the inclusion of additional standards with regard to CTPs’ cyber security, governance, and supply chain risk management.

5.4 In response to DP3/22, the regulators propose:

- not to include Operational Risk and Resilience Requirements dealing with:
 - ‘Identification’ for the reasons discussed in Chapter 5 or
 - ‘Testing’ as it would unnecessarily duplicate the proposed requirements and expectations on ‘Information-Gathering and Testing’ in Chapter [6];
- to make ‘Engagement with the supervisory authorities’ one of the proposed CTP Fundamental Rules (see Chapter [4]);
- to merge the standards on ‘Financial sector continuity playbook’ and ‘Post-incident communication’ in DP3/22 into a single Operational Risk and Resilience Requirement (renamed ‘Incident Management’);
- to apply the concept of ‘Learning and Evolving’ throughout the proposed requirements and expectations for CTPs rather than keeping it as a standalone requirement;
- introduce new Operational Risk and Resilience Requirements on dependency and supply chain risk management, technology and cyber resilience, and change management; and
- introduce proposed incident notification requirements for CTPs (see Chapter 7).

Proposed CTP Operational Risk and Resilience Requirements

5.5 The aim of the proposed Operational Risk and Resilience Requirements is to provide clear and consistent obligations that all CTPs would be required to meet in respect of their material services.

5.6 Although the proposed CTP Operational Risk and Resilience Requirements are more granular than the proposed CTP Fundamental Rules in Chapter 4, they are still

outcomes-focused. They specify objectives that CTPs would have to achieve in respect of their material services, but do not propose to prescribe how they should be met.

5.7 Although a CTP should manage all relevant risks as part of its overall risk management processes under Requirement 2, there are three specific areas that the regulators propose to address explicitly and individually in Requirements 3 to 5 respectively, given their importance and relevance to the oversight regime for CTPs. These areas include dependency and supply chain risk management, technology and cyber resilience, and change management.

Requirement 1: Governance

5.8 The regulators propose to require every CTP to ensure that its governance promotes the resilience of its material services by:

- appointing an appropriately-qualified employee of the CTP (or member of its governing body) who has the appropriate authority, knowledge, skills, and experience, to act as the central point of contact with the regulators in their capacity as authorities having oversight functions;
- establishing clear roles and responsibilities at all levels of its staff involved in the delivery of material services, with clear and well-understood channels for communicating and escalating issues and risks;
- establishing, overseeing, and implementing an approach that covers the CTP's ability to:
 - prevent, respond, and adapt to, as well as recover from any event that causes disruption to the delivery of a material service; and
 - learn from those events and any testing undertaken; and
- ensuring appropriate review and approval of any information provided to the regulators.

5.9 The regulators also propose to require a CTP to notify them in writing of the name of the appointed person, their business address, and other up to date contact details including email addresses, telephone numbers, and out of hours contact details.

5.10 In the draft supervisory statement, the regulators set out their proposed expectations of what would constitute appropriate review and approval of information.

Requirement 2: Risk management

5.11 The regulators propose to require each CTP to effectively manage risks to its ability to continue to deliver a material service by:

- identifying and monitoring relevant external and internal risks;

- ensuring that it has risk management processes that are effective at managing those risks, and;
- regularly updating its risk management processes to reflect lessons learned and issues arising from:
 - a disruption to a material service;
 - engagement with regulators;
 - new and emerging risks; and
 - any associated testing, including but not limited to testing carried out in accordance with the proposals in Chapter 6 of this CP.

5.12 Many risks to a CTP's delivery of material services are likely to be operational. The draft Supervisory Statement sets out a non-exhaustive list of examples. However, the regulators propose that a CTP should also consider financial risks that may affect its ability to deliver material services, such as the risk of insolvency.

5.13 To comply with Requirement 2, the draft supervisory statement proposes that a CTP would be expected to have a sound risk management framework to manage risks to the delivery of material services. The regulators expect that such a framework would include:

- strategies, policies, and procedures to identify, measure, monitor, and report on relevant risks (including a risk appetite);
- policies and procedures to control and manage risks within the CTP's risk appetite; and
- mechanisms to periodically review and ensure that the strategies, policies, and procedures referred to above were designed and operating effectively.

5.14 A CTP would also be expected to monitor risks on an ongoing basis, including through horizon scanning and the use of threat intelligence.

Requirement 3: Dependency and supply chain risk management

5.15 The regulators propose to require each CTP to identify and manage any risks to its supply chain that could affect its ability to deliver material services. A CTP must take all reasonable steps to ensure that each person in its supply chain:

- understands the requirements that apply to the CTP by virtue of the 'CTP duties' (which is an umbrella term in the regulators' draft rules covering all the duties and obligations placed upon a CTP by or as a result of the FSMA, including the proposed rules and any equivalent rules of the other Regulators);
- acts to facilitate the CTP meeting those requirements; and

- provides the regulators with access to any information relevant to them exercising their oversight functions.

5.16 Although a CTP would be required to manage all risks as part of its overall risk-management under Requirement 2, dependency and supply chain risks have unique characteristics that merit individual consideration. It is particularly important that a CTP ensures that entities that are essential to its delivery of material services to firms and FMIs meet certain resilience outcomes. Consequently, although separate, the proposed requirements in Requirement 3 would apply as part of a CTP's risk management under Requirement 2. In line with the principle of proportionality (and consistent with the FSB TPR toolkit), when managing dependency and supply chain risks CTPs should focus on Key Nth party service providers (as defined in section 2) and other parts of their supply chain that are knowingly essential to the delivery of material services to firms and FMIs, or which have access to confidential or sensitive data belonging to the firms and FMIs.

5.17 To comply with Requirements 2 and 3, the regulators propose in the draft supervisory statement that a CTP would be expected to:

- perform appropriate due diligence before entering into sub-contracting arrangements that are key to its delivery of material services and monitor these arrangements on an ongoing, or regular (at least annual) basis thereafter;
- be transparent with the regulators and its firm and FMI customers about which parts of its supply chain are essential to its delivery of material services;
- obtain appropriate information about incidents in its supply chain;
- include scenarios involving supply chain disruption in its testing; and
- incorporate lessons learned from disruption to and testing of its supply chain into its risk management and incident management processes (see Requirements 3 and 7).

Requirement 4: Technology and cyber resilience

5.18 The regulators propose to require a CTP must ensure the resilience of any technology that delivers, maintains or supports a material service, including by having:

- technology and cyber risk management and operational resilience measures;
- regular testing of those measures (including as part of the requirements examined in Section 6);
- processes and measures that reflect lessons learned from testing; and
- processes and procedures that convey relevant and timely information to assist risk management and decision-making processes.

5.19 A CTP would be required to meet the proposed requirements on technology and cyber resilience in Requirement 4 as part of compliance with the wider risk management processes under Requirement 2.

5.20 The regulators consider that, like dependency and supply chain risk management and change management (examined below), technology and cyber resilience merits being explicitly considered under the proposed Requirements due to its technical complexity. In addition, over the past few years, the risk of a cyber-attack has been consistently identified in the Bank's biannual [Systemic Risk Survey](#) as the top or one of the top risks that would have the greatest impact on the UK financial system if it were to materialise (see Chart 4 in [Systemic Risk Survey Results – 2023 H2](#)).

5.21 To facilitate compliance with Requirement 4, in the draft supervisory statement the regulators propose a range of additional expectations setting out what a CTPs technology and cyber resilience measures should include.

5.22 Finally, the regulators propose that a CTP should ensure that cyber and technology response and recovery measures are considered as part of compliance with Requirement 7: incident management.

Requirement 5: Change management

5.23 The regulators propose to require a CTP to ensure it has a systematic approach to dealing with changes to a material service (including changes to the processes or technologies used to deliver, maintain, or support that service) by:

- implementing appropriate policies, procedures, and controls to ensure the resilience of any change to a material service;
- implementing any change to a material service in a way that minimises the risk of undue disruption; and
- ensuring that prior to being implemented, any change is appropriately risk-assessed, recorded, tested, verified, and approved.

5.24 To comply with Requirement 5, the regulators propose that a CTP should assess the evolution of risk throughout the change process from inception to termination in the draft supervisory statement. The draft supervisory statement sets out a non-exhaustive list of the types of change the regulators propose that CTPs should consider.

5.25 The regulators propose that before commencing a change to a material service, a CTP should plan what it will do if the change fails. This may include but would not be limited to reversing or rolling back the change.

5.26 The regulators also propose that CTPs should continue to monitor changes to material services for an appropriate period after their implementation to identify and manage any unexpected risks.

Requirement 6: Mapping

5.27 The regulators propose to require a CTP to:

- subject to transitional arrangement and the bullet below identify and document:
 - resources including the assets and technology used to deliver, support, and maintain each material service it provides; and
 - any internal and external interconnections and interdependencies between the resources identified in respect of that service.
- have completed the identification and documentation of the set resources within 12 months of being designated by HMT, and keep it up to date at all times thereafter.

5.28 Mapping is a key concept in the operational resilience framework for firms and FMI and in the BCBS Operational Resilience Principles. Respondents to DP3/22 welcomed the idea of adapting mapping requirements to CTPs. Some respondents questioned how granular CTPs' maps would be expected to be, and others suggested that mapping should include dependencies and vulnerabilities across all material services.

5.29 The key objectives of mapping in its proposed application to CTPs would be to enable a CTP to identify vulnerabilities (which should then inform its scenario testing) by:

- distinguishing those resources across the supply chain that are essential to the CTP's delivery of material services and any interconnections between them (the draft supervisory statement contains a non-exhaustive, illustrative list of resources);
- ascertaining whether these resources are fit for purpose; and
- considering what would happen if they became unavailable.

5.30 The regulators do not propose to require CTPs to use a set format for their map(s), but would expect the maps produced by CTPs to:

- focus on resources that are essential to the CTP's delivery of material services;
- be sufficiently granular to meet the objective set out above; and
- be updated annually or following certain events (eg a change to a key nth party supplier).

Requirement 7: Incident management

5.31 The regulators propose to require that a CTP appropriately manages incidents that adversely affect, or may reasonably be expected to adversely affect, the delivery of a material service including by:

- implementing appropriate measures to respond to and recover from incidents in a way that minimises the impact;
- setting a maximum tolerable level of disruption to the service;
- maintaining and operating a Financial Sector Incident Management Playbook; and
- coordinating and engaging with arrangements put in place by firms, FMIs, authorities or other persons for coordinating responses to incidents affecting the UK's financial sector. In this context 'authorities' may include:
 - the authorities participating in the [Authorities' Response Framework \(ARF\)](#);
 - non-UK financial regulatory, oversight or supervisory authorities such as (where applicable) the CTP's lead overseer under DORA;
 - regulators and other public authorities outside the financial services sector, which may have an overlapping mandate or interest in respect of the CTP.

Response and Recovery Measures

5.32 In the draft supervisory statement, the regulators propose that a CTP's response and recovery measures should cover the lifecycle of an incident, including but not limited to:

- the setting of a maximum tolerable level of disruption for the material service prior to the incident occurring;
- the classification of incidents based on predefined criteria eg expected recovery time, and (if known) potential impact on the CTP's firm and FMI customers;
- procedures and targets for restoring material services and recovering data eg recovery time objectives (RTOs), recovery point objectives (RPOs) etc. To the extent possible, these targets should be compatible with the impact tolerances that firms and FMIs have set for any important business services, which are in turn supported by the CTP's relevant material services;
- internal and external communication plans; and
- continuous improvement through the incorporation of lessons learned from previous incidents and testing.

5.33 The draft supervisory statement sets out further proposals for how a CTP should set a maximum tolerable level of disruption, including the use of appropriate metrics and targets.

5.34 The regulators propose that a CTP would also be expected to:

- periodically, and at least annually, test and update its response and recovery measures; and
- identify the root causes of incidents and take all reasonable steps to address them to reduce the risk of incidents reoccurring.

5.35 The regulators propose that a CTP's response and recovery measures should cover incidents with a potential cross-border and cross-sectoral impact.

Financial sector incident management playbooks

5.36 In line with responses to DP3/22, the primary objective of financial sector incident management playbooks would be for a CTP to consider, plan, document, test, and regularly review how it would communicate with and support the regulators, and its firm and FMI customers (collectively and individually) during an incident affecting one or more of its material services.

5.37 The regulators recognise that each incident will be different, and there can be no one-size-fits-all approach. However, the regulators propose that the playbook should meet a number of outcomes, including setting out how a CTP would:

- coordinate its crisis communications with those of the firms and FMIs to which it provides material services in order to mitigate risks to the stability of, and confidence in, the financial system; and
- ensure that its firm and FMI customers and the regulators receive accurate, consistent, and timely information and support throughout the incident's lifecycle.

5.38 To comply with Requirement 7 and the proposed requirements on information-gathering and testing in Chapter 6 of this CP, the regulators propose to require a CTP to test its financial sector incident management playbook at least annually with an appropriately representative sample of firms and FMIs to which it provides a material service (see Chapter 6).

5.39 The regulators propose that a CTP should make its financial sector incident management playbook available to them on request.

Engagement with arrangements for coordinating responses to incidents affecting the financial sector

5.40 The regulators propose to require that a CTP engages with arrangements put in place by firms, FMIs, authorities, or other persons for coordinating responses to incidents affecting the UK's financial sector. The Bank's webpage on [Operational resilience of the financial sector](#) mentions some of these arrangements, which include but are not limited to the Cross Market Business Continuity Group (CMBCG), the [Financial sector cyber collaboration centre \(FSCCC\)](#), and the Sector Response Framework (SRF). The regulators do not propose to prescribe specific financial sector incident response frameworks that the CTP must engage with.

5.41 The regulators' proposed requirements on incident notification (set out in Chapter 7) would include a requirement on CTPs to name an individual who would be responsible for communicating with the firms to which the CTP provides services about the relevant incident in their initial incident notifications. The regulators propose that this individual should also be responsible for communicating arrangements for coordinating responses to incidents affecting the financial sector.

Requirement 8: Termination of services

5.42 The regulators propose to require a CTP to have in place appropriate measures to respond to a termination of any of its material services, including by putting in place:

- arrangements to support the effective, orderly, and timely termination of those services, including (if applicable) their transfer to another person, including the firms or FMIs the services are provided to; and
- provision for ensuring access, recovery and return of any relevant assets to the firms or FMIs it provides the material service to (and where applicable in an easily accessible format).

5.43 The draft supervisory statement sets out a non-exhaustive range of reasons why termination could happen, including but not limited to corporate restructuring, change in control, legal or regulatory issues, insolvency, court processes, or unrecoverable disruption. Firms and FMIs would remain responsible for complying with applicable requirements and expectations on operational resilience and third-party risk management, including in relation to stressed exits. The measures that CTPs should take under Requirement 8 seek to facilitate firms' and FMIs' compliance with these requirements.

6: Information-gathering, self-assessment, testing, Skilled Person Review and information sharing

6.1 The regulators propose to require CTPs to comply with a range of information-gathering and testing requirements in:

- the regulators' information-gathering power under s312P FSMA;
- Chapter 11 and 12 of the Critical Third Parties sourcebook in the FCA Handbook; and
- the following chapters in the Critical Third Parties Parts of the PRA and Bank Rulebooks:
 - information-gathering, evidence and testing;
 - self-assessment; and
 - information sharing with firms.

6.2 In Chapter 6 of DP3/22, the regulators set out a potential approach to testing the resilience of services that CTPs provide to firms and FMIs using a range of tools, including but not limited to:

- scenario-testing;
- participation in sector-wide exercises, such as: FPC cyber stress tests, Sector Simulation Exercises (SIMEX), and Quantum Dawn;
- cyber-resilience testing; and
- skilled persons reviews.

6.3 This section of the DP attracted a large number of responses. Respondents to the DP generally supported the regulators' thinking but encouraged them to:

- adopt an agile, proportionate approach to testing the resilience of CTPs, which leveraged a wide range of available tools; and
- take into account CTPs' own testing (whether performed internally or by independent parties); and other forms of oversight carried out by other regulators and authorities.

6.4 Respondents also recognised the potential value of bringing CTPs into sector-wide exercises but raised concerns about the resources and time involved in organising them. As an alternative, some respondents suggested that CTPs could be required to

run smaller, similar exercises with volunteers from the firms and FMIs to which they provide services.

6.5 There were mixed views about the potential value of the regulators performing threat-led penetration testing on CTPs. Respondents also noted the importance of ongoing monitoring and vigilance by CTPs, and appropriate follow-up by the regulators of any recommendations for remediation resulting from tests or other forms of oversight.

6.6 The regulators have taken responses to DP3/22 into account when developing the proposed requirements and expectations on assurance, information gathering and testing of CTPs in this chapter.

General evidence and information requirement

6.7 The regulators propose a general requirement for every CTP to demonstrate to the regulators its ability to comply with their rules both annually and upon request.

Self-assessment

6.8 The regulators propose to require each CTP to submit a written self-assessment to the Regulators within three months of designation and thereafter within 12 months of the last submission. The self-assessment would be expected to include the information in Box 2 of the draft supervisory statement. A CTP would also be expected to make any documents referenced in the self-assessment available to the regulators upon request (eg independent assurance reports, certifications etc). The regulators propose to require CTPs to keep a copy of their self-assessment for at least three years. In line with CTP Fundamental Rule 6, the regulators would expect CTPs' self-assessments to be balanced, thorough and transparent. In particular, they should openly highlight identified vulnerabilities, areas for improvement and proposed remediation. CTPs should use factual language and avoid an undue 'good news culture' when completing their self-assessments.

Testing requirements

Scenario testing

6.9 Under the regulators' proposals, a CTP would be required to:

- carry out regular scenario testing of its ability to continue providing each material service within its maximum tolerable level of disruption in the event of a severe but plausible disruption.

- identify an appropriate range of adverse circumstances of varying nature, severity, and duration relevant to its business, risk profile, and supply chain and consider the risks to the delivery of the material service in those circumstances.

6.10 The proposed scenario testing requirements and expectations for CTPs are adapted from the requirements and expectations in the operational resilience framework for firms and FMIs. CTPs would be expected to assume that disruption is inevitable when designing their scenarios for testing.

6.11 The regulators would expect the sophistication of a CTP's scenario testing to be consistent with its systemic significance while balancing minimising the risk of disruption to its operations or customers.

Testing financial sector incident management playbooks

6.12 The regulators propose to require a CTP to test its financial sector incident management playbook annually. If justified, the regulators could also direct a CTP to re-test its playbook at a different time or more frequently than once a year. For instance, following significant disruption. The regulators would expect the testing to:

- be organised and coordinated centrally by the CTP;
- include an appropriate representative sample of the CTP's firm and FMI customers to which it provides material services; and
- be reviewed and approved at an appropriate level in the CTP.

6.13 The regulators also propose to require each CTP to produce a report following each test of its financial sector incident management playbook and share it with the regulators. The report should be completed as soon as reasonably practicable and sent to the regulators immediately after the report is completed. The report would be expected to set out:

- the key findings from the test;
- proposed revisions to the CTP's Financial Sector Incident Management Playbook or the CTP's incident management more broadly; and
- general non-attributable feedback to the CTP's firm and FMI customers based on the test eg on best practices identified.

Information on request

6.14 In addition to the proposed annual self-assessment and testing requirements, the regulators could ask a CTP to provide information under s312P FSMA if reasonably required. The draft supervisory statement sets out expectations regarding how CTPs should comply with these requests.

Skilled person reviews

6.15 Under s166(3) FSMA, any of the regulators may require a CTP or any person connected with a CTP to appoint, or the regulators may appoint, a skilled person to provide the regulators with a report. Similarly, under s166(A)(2) FSMA, each of the regulators may also require a CTP or any person connected with a CTP to appoint, or may itself appoint, a skilled person to collect or update information.

6.16 The regulators may use s166 reviews for any purpose in connection with their functions, including for resilience testing. The regulators' proposed approach to the exercise of their powers to order skilled persons reviews of CTPs is consistent with existing obligations on firms and FMIs, and is set out in:

- Chapter 12 of the Critical Third Parties sourcebook in the FCA Handbook;
- the 'Cost of Skilled Persons Reviews' and 'Contracts with Skilled Persons and delivery of reports' chapters in the Critical Third Parties Parts of the PRA and Bank Rulebooks; and
- a separate draft supervisory statement.

Cost of appointing a Skilled Persons

6.17 A CTP or the person connected with a CTP shall pay the cost of a skilled persons review where the skilled person is appointed by the CTP or the person connected with a CTP. Where a regulator appoints the skilled person, the regulators have proposed a rule that all the expenses incurred by the regulator in relation to that appointment shall be payable to it by the CTP or the person connected with a CTP. This follows the existing requirements in place for firms and FMIs with respect to paying for S166 reviews.

Contracts with Skilled Persons and Delivery of Reports

6.18 The regulators propose a range of contractual requirements that must be fulfilled when a CTP contracts with a skilled person. In particular, the CTP would be required to permit the skilled person during and after the course of their appointment to:

- cooperate with the regulators in the discharge of their oversight functions;
- communicate to the regulators:
 - information on, or their opinion on, those matters that may be of material significance to the regulators in determining whether the CTP concerned satisfies and will continue to comply with their CTP duties;

-
- information or their opinion on whether they reasonably believe that the CTP is not, may not be, or may cease to be a going concern;
 - require the skilled person to prepare a report or collect or update information, as notified to the CTP by the regulator, within the time specified by the regulators; and
 - waive any contractual or other duty of confidentiality owed by the skilled person to the CTP which might limit the provision of information or opinion by that skilled person to the regulators.

6.19 The regulators propose to require a CTP to ensure that the contract requires and permits the skilled person to provide the regulators with:

- interim reports;
- source data, documents, and working papers;
- copies of any draft reports given to the CTP; and
- specific information about the planning and progress of the work to be undertaken (which may include project plans, progress reports including percentage of work completed, details of time spent, costs to date, and details of any significant findings and conclusions).

6.20 The regulators propose that the s166 contract must be:

- governed by the laws of a part of the UK;
- in writing; and
- include a number of enforcement and arbitration provisions.

6.21 The regulators propose that when a CTP appoints a skilled person (either directly or indirectly), the CTP would be required to take reasonable steps to ensure that the skilled person delivers a report or collects or updates information in accordance with the terms of appointment.

6.22 The regulators also propose that a CTP must provide all reasonable assistance to a skilled person appointed under section 166 or 166A and take reasonable steps to ensure that its employees and agents do so.

Sharing of assurance and testing information with firms and FMIs

6.23 The regulators propose to require every CTP to have in place effective and secure processes and procedures to ensure that their firms and FMI customers can comply with their regulatory obligations, and adequately manage risks related to their use of the CTP's services. CTPs would be required to share:

- the results of scenario testing described in paragraph 6.9 above and financial sector incident management playbook testing described in paragraph 6.12 above with the regulators' requirements, including any recommended remediation (where that information relates to a firm to which it provides services); and
- a summary of the information contained in the CTP's annual self-assessment submitted to the regulators.

6.24 The regulators propose that a CTP would be responsible for developing an appropriate method for sharing these summaries and other information with its firm and FMI customers. This method should include controls to ensure that confidential or sensitive information is appropriately protected.

7: Notifications

7.1 The regulators propose to require CTPs to notify them and their firm and FMI customers who receive an affected service of certain incidents. The proposed requirements are in:

- Chapter 8 of the Critical Third Parties sourcebook in the FCA Handbook; and
- the 'Notifications' and 'Inaccurate, False or Misleading Information' chapters in the Critical Third Parties Parts of the PRA and Bank Rulebooks.

7.2 Where a CTP would be required to disclose information under the regulators' rules that would be subject to s413 of FSMA (which deals with information subject to legal privilege), this information is not disclosable to the regulators. However the CTP may choose whether or not to disclose this information to firms.

7.3 The DP addressed post-incident communications. In line with responses to the DP, the regulators consider that incident notification requirements for CTPs are necessary to advance the objectives of the regime.

7.4 The proposed rules on incident notification would supplement CTP Fundamental Rule 6 with specific incident notification requirements for CTPs. The combined purpose of these proposed requirements is for the regulators and a CTP's firm and FMI customers to receive consistent, sufficient, and timely information about incidents affecting a CTP's material services throughout the lifecycle of these incidents in order to:

- assess the potential impact of these incidents on the stability of, and confidence in, the UK financial system; and
- implement response and recovery measures both at the individual firm and FMI level, and on a coordinated sector-wide level.

7.5 Firms would continue to be subject to the explicit and implicit incident notification requirements in PRA Fundamental Rule 7, Principle 11 of the FCA Principles for Businesses, and the general notification requirements in the [FCA's](#) and [PRA's](#) respective rules. Similar requirements or expectations also apply to FMIs. These requirements on firms and FMIs will apply in addition and without prejudice to the proposed incident notification requirements for CTPs.

Relevant incident

7.6 The incident notification proposals would apply to the notification of a 'relevant incident', which is defined as either a single event or a series of linked events that actually or has the potential to:

- seriously disrupt the delivery of a material service; or
- seriously and adversely impact the availability, authenticity, integrity or confidentiality of assets relating or belonging to the firms which the CTP has access to as a result of it providing services to firms or the potential to result in a serious loss of such assets.

7.7 A relevant incident could result from one or more events. These events could be planned, unplanned. Unplanned events could include a cyber-attack or a natural disaster. A planned event, such as a software update or change management programme (see chapter five), could also lead to a relevant incident if it gave rise to the types of disruption and or failure referred to above. A combination of planned and unplanned events could also lead to a relevant incident.

Phased approach to incident notifications

7.8 The regulators propose to require a CTP to provide, the following notifications to both the firms and FMI it provides services to, and to the regulators

- an initial incident notification;
- one or more intermediate incident notifications; and
- a final incident notification.

7.9 The CTP should in all cases provide these notifications based on its reasonable knowledge at the time of submission.

7.9 The regulators propose to require a CTP to also provide additional information about the incident to the regulators if requested pursuant to the information-gathering powers in s312P FSMA.

7.10 The regulators' proposed phased and incremental approach to incident notifications by CTPs is aligned to the FSB's [Recommendations to Achieve Greater Convergence in Cyber Incident Reporting](#) ('FSB CIR Recommendations'), which the regulators also propose to extend to incidents in general, not just cyber-incidents.

Format of incident notifications

7.11 A CTP would be able to use a range of formats for their notifications as long as they include the information specified in the regulators' draft rules and draft supervisory statement. As included in the [Regulatory Initiatives Grid](#), the regulators are developing a new approach to incident reporting for firms and FMIs. This project was chosen as a phase two use case as part of the [Transforming Data Collection Programme](#).

7.12 The regulators propose that the CTP can use updates to other customers or authorities as notifications so long as they include the information referred to in chapter seven of the draft supervisory statement at a minimum.

Incident notification triggers and initial incident notification

7.13 The regulators propose that a CTP must submit an initial notification without undue delay after the CTP is aware that the relevant incident has occurred.

7.14 The regulators propose that the initial notification to the firms and FMIs the CTP provides services to and the initial notification to the regulator must include the

information specified in the draft rules. These draft rules include additional data to be submitted to the regulators based on the relevant incident's potential impact on the stability of, or confidence in, the UK's financial system (likewise based upon the CTP's reasonable knowledge at the time of the submission).

7.15 Once the regulators receive an initial incident notification from a CTP, they will consider the most appropriate form of follow-up on a case-by-case basis. When doing so, the regulators will coordinate and share information with other authorities, subject to appropriate information-sharing arrangements such as memoranda of understanding, for example: HMT, non-UK financial authorities and UK non-financial authorities, including the NCSC if the incident is a cyber-incident.

Intermediate incident notifications

7.16 The main purpose of intermediate incident notifications would be to assist the regulators, and the CTP's firm and FMI customers in their response and recovery, by updating them on further developments relating to the incident and its potential implications (including new information that may have come to light since the initial incident notification).

7.17 The regulators propose that a CTP periodically provide intermediate incident notifications, based upon its reasonable knowledge at the time of submission. However, the frequency, level of detail and timing of submission of these intermediate notifications should balance the competing needs of the:

- regulators, firms and FMIs to be updated on the evolution of the incident; and
- CTP to prioritise the implementation of its response and recovery measures.

7.18 Under this proposal, if a CTP resolves an incident before an intermediate notification is due, it can move straight to the financial incident notification phase. The CTP should, however, let the regulator know that the incident has been resolved as soon as reasonably practicable and follow-up with the final incident notification thereafter.

Final incident notification

7.19 Once a relevant incident has been resolved and the CTP has had time to assess its root causes and identify lessons learned, the regulators propose that it must provide a final incident notification to the regulators, and the firms and FMIs it provides services to. The proposed contents of the final notification are set out in the regulators' draft rules.

Other notification requirements

7.20 In addition to the incident notification requirements examined in the previous sections, the regulators propose to require CTPs to notify them if:

- civil proceedings are brought by or against the CTP or a claim or dispute is referred to alternative dispute resolution, in any jurisdiction, and it poses a significant threat to the CTP's reputation or ability to provide any material service.
- the CTP enters into any form of alternative dispute resolution (e.g. arbitration, mediation etc.) that poses a significant threat to the areas referred to in the previous bullet point;
- the CTP is subject to criminal proceedings, has been prosecuted for, or has been convicted of, a criminal offence in any jurisdiction involving fraud or dishonesty;
- disciplinary measures or sanctions have been imposed on the CTP by any statutory or regulatory authority in any jurisdiction (other than the Regulators) or the CTP becomes aware that one of those bodies has commenced an investigation into its affairs;
- the CTP is in financial difficulty and is considering entering into an insolvency proceeding or a restructuring plan in any jurisdiction or proceedings are likely to be brought against it in any jurisdiction;
- there is an actual or potential circumstance or event that seriously and adversely impacts the CTP's ability to meet its CTP duties.

8: Misleading use of designation status

Public references to a CTP's designated status

8.1 Responses to DP3/22 highlighted the risk that CTP designation could be misinterpreted as a regulatory 'kite-mark' of approval. Respondents felt that firms and FMIs may be more likely to contract with a CTP over a non-designated third party providing similar services on the assumption that the CTP is more resilient, or that this would be encouraged by the regulators.

8.2 This consultation package makes clear that designation does not mean a third party has superior operational resilience to a non-designated third party and is not inherently safer than non-designated third parties. As we explain in chapter 2, the regulators will recommend CTPs for designation based on criteria relating to concentration in and materiality of the services they provide to firms and FMIs. They will not be hand-picked as favoured, operationally resilient suppliers. The regulators have also emphasised that ultimate accountability and responsibility for firms' outsourcing and operational resilience obligations cannot be outsourced to a CTP. The proposals would not change the fact that financial services firms need to conduct due diligence and perform ongoing monitoring of third parties they engage, whether these be designated CTP or otherwise. Moreover, contracting with a CTP would not relieve a firm or FMI from liability in any potential enforcement action.

8.3 Nevertheless, the regulators recognise the risk of firms misinterpreting designation as regulatory approval and the potential for CTPs to encourage this. The regulators therefore propose to prevent a CTP from unduly using its designation for marketing purposes.

8.4 Under this proposal, a CTP would be required to refrain from indicating or implying that it has the approval or endorsement of the regulators by virtue of its designation as a CTP or being overseen by the regulators in respect of services it provides to firms or FMIs. Likewise, the regulators propose that a CTP must not suggest in any communication that its designation by HMT or oversight by the regulators confers any advantage to a firm or anyone else in using its services as compared to a service provider who is not designated. The regulators also recognise the potential for some related competition impacts, which are discussed in the CBA in Appendix 6.

8.5 The relevant draft rules are located in:

- Chapter 13 of the Critical Third Parties sourcebook in the FCA Handbook; and
- the 'Referrals to oversight by the regulators or designation by HMT' chapters of the Critical Third Parties Parts of the PRA and Bank Rulebooks

9: Nomination of a legal person for non-UK CTPs

Nomination of a legal person

9.1 As noted earlier, the focus of the proposals in this CP is on the services that a CTP provides to firms and FMIs. Consequently, the proposals are agnostic about the location of CTPs and do not require them to set up an establishment (ie a branch or subsidiary) in the UK where one does not already exist. This approach recognises that many CTPs provide services across international borders and/or to clients in multiple jurisdictions, and that this can help improve the efficiency and resilience of firms and FMIs and reduce compliance costs for CTPs.

9.2 However, for practical purposes, in addition to the proposed requirements in Requirement 1 of the operational risk and resilience chapter of the draft rules, a CTP whose head office is outside the UK would be required to nominate a legal person with authority to receive documents and notices from the regulators (including statutory notices under FSMA). The term 'person' is as defined in Schedule 1 of the Interpretation Act 1978 and 'includes a body of persons corporate or unincorporate'. For the purposes of this requirement, the regulators propose that a CTP with no presence or employees in the UK should appoint a law firm or other suitable UK-based corporate body, partnership, or limited liability partnership as its representative.

9.3 The relevant rules are located in:

- Chapter 10 of the Critical Third Parties sourcebook in the FCA Handbook; and
- the Nomination chapters of the Critical Third Parties parts of the PRA and Bank Rulebooks.

10. Record keeping and emergency relief

10.1 The regulators propose that a CTP must arrange for orderly records to be kept of its business and internal organisation, in so far as it concerns the provision of services

to firms or FMIs. These records must be sufficient to enable each regulator to perform its oversight functions; and to ascertain whether or not the CTP has complied with its duties.

10.2 The relevant rules are located in:

- Chapter 14 of the Critical Third Parties sourcebook in the FCA Handbook; and
- the Nomination chapters of the Critical Third Parties Parts of the PRA and Bank Rulebooks.

Emergency

10.3 Bank draft rules include proposals that are intended to provide relief to a CTP in an emergency circumstance when it would be impossible for the CTP and related persons to comply with the proposed rules.

10.4 The relevant draft rules are located in the Critical Third Parties Emergency Provisions Part of the Bank rulebook.

10.5 The PRA and FCA do not need to propose emergency rules because the equivalent existing rules in the General Provisions part of the PRA rulebook and the **FCA Handbook** apply to a 'person' which includes a CTP.

11: Regulators' statutory obligations

11.1 In this chapter, the regulators address their statutory obligations in relation to the proposals in this CP.⁶ These obligations, which include regulatory objectives, 'have regards' and duties, are in some cases shared across more than one of the regulators. In other cases, they apply to just one regulator. Where the obligations are shared across two or more regulators, the analysis is combined.

Regulators' objectives analysis

PRA primary objective: safety and soundness

11.2 The PRA considers that the proposals would advance the PRA's primary objective of promoting the safety and soundness of the firms it supervises by helping to increase the long-term system-wide resilience of the financial sector. PRA-regulated firms are becoming increasingly dependent on certain services provided by third parties for the delivery of their important business services. Failure or disruption to the services that certain third parties provide to PRA-regulated firms could impact these firms' ability to continue providing important business services within their impact tolerances. This could in turn jeopardise the safety and soundness of these firms (potentially simultaneously or in short succession) and, in some instances, threaten the stability of, or confidence in, the UK financial system. Moreover, as previously highlighted by the FPC, the regulators, and the FSB, no single firm can adequately manage the risks stemming from concentration on a third party, or a small number of third parties, for the provision of material services to multiple firms. Additional regulatory measures are therefore needed to address the potential systemic risks posed by the financial sector's growing dependence on third parties and deliver the PRA's primary objective.

PRA primary objective: insurance policyholder protection

11.3 The PRA considers that the proposals in this CP are compatible with, and would advance, the PRA's insurance objective. The third parties designated as CTPs under the proposed regime could include those who provide material services to insurers. The proposed measures would allow the regulators to mitigate and manage risks that could

⁶ Some statutory obligations and have regards are not yet in force at the time of the publication of this CP. They are considered in this CP on the basis that the publication of final policies and rules will take place after these relevant obligations come into force and because the duty to consult can be satisfied by things before (or after) that date pursuant to s.81 FSMA 2023.

arise from a failure in or disruption to these services and cause downstream harm to insurance policyholders.

Bank of England primary objective: financial stability

11.4 The Bank considers that the proposals in this CP would advance its primary objective of promoting the stability of the UK's financial system. FMIs are becoming increasingly dependent on certain third parties, such as technology service providers, for their delivery of functions that are vital to the financial stability of the UK. Multiple FMIs using the same third party can represent a concentration risk that may pose a threat to the vital services those FMIs provide to the financial system. FMIs in particular can often be the sole provider of services – such as clearing, settlement and payment services - that are vital to the functioning of the UK financial markets and hence to UK financial stability. FMIs may rely on third parties for critical components of these services.

FCA strategic objective and FCA operational objective: integrity

11.5 Firms and FMIs are becoming increasingly dependent on certain third parties to deliver functions that are vital to the UK financial system. The proposals aim to mitigate the risks arising by improving the resilience of such third party services which support the UK financial system. As explained in the CBA, the regulators have also sought to prevent the proposals inadvertently entrenching the market power of incumbent third parties, and thereby avoid increasing risk to the UK financial system. As such, the FCA considers that the proposed regime advances its strategic objective of ensuring that the relevant markets function well and the objective of protecting and enhancing the integrity of the UK financial system.

FCA operational objective: consumer protection

11.6 The FCA considers that the proposals advance the FCA's objective of securing an appropriate degree of protection for consumers. While the policy proposals do not impact consumers directly, the FCA considers that the proposed policy will benefit them through the reduction of systemic risk to the wider financial system. The reduction of systemic risk should reduce harm to consumers since where firms are reliant on third parties, services these firms provide to consumers should benefit from reduced instances of disruption and failure, and thus negative impact. The regulators explain in the CBA that the competition impact of the proposals resulting in any pass through of costs to end consumers would depend on supply and demand elasticities.

Bank of England's secondary innovation objective and FCA and PRA have regard to innovation in HMT's remit letters

11.7 The Bank considers that this policy accords with the Bank of England's secondary objective, in exercising its FMI functions to advance the primary stability objective, to facilitate innovation in the provision of FMI services so far as reasonably possible. The PRA and FCA also consider that this policy accords with their respective have regard to innovation in HMT's remit letters.

11.8 The regulators note that the proposals will not place any requirements on firms or FMIs themselves around the use of CTPs for provision of services, and also does not change the incentives for firms or FMIs with respect to their use of CTPs for provision of services. Moreover, the regime does not discriminate on the basis of particular technologies – the policy is intended to be technology-neutral and focuses on regulatory outcomes.

11.9 The CBA acknowledges the potential competition impacts of the regime, which could in turn affect innovation. However, as explained in the CBA, the regulators consider that these impacts are unlikely to be material.

Statutory obligations relating to competition

PRA and FCA competition 'have regard' in Treasury remit letters

11.10a The proposals engage the PRA and FCA competition 'have regard', which suggests that the PRA and FCA should consider competition in relation to 'all consumers'. This may include any 'upstream' impact resulting from competition among CTPs. Accordingly, in the CBA, the regulators have considered not only competition among CTPs, but also the potential for the proposals to have indirect competition impacts on firms and end consumers. As set out in the CBA, where the regulators believe that there are potential impacts, like the 'halo effect', these are mitigated as described or in other cases these potential impacts are unlikely to be material. The regulators therefore consider the proposals to be compatible with the PRA and FCA competition 'have regard'.

PRA secondary objective: competition

11.10b The regulators consider that while the proposals in this CP are compatible with the PRA's secondary competition objective, they are not expected to have a direct impact on the market for services provided by PRA regulated firms. The proposals are directed at CTPs and will not place new burdens or obligations on existing PRA-

authorised firms. Potential impacts on competition are considered more fully in the CBA.

FCA operational objective: competition and competition duty

11.11 The proposals are directed at CTPs and will not place new burdens or obligations on existing FCA-authorized firms. They do not directly impact competition within the relevant markets under the FCA's competition objective. Likewise, the FCA's competition duty relates to 'effective competition in the interests of consumers'. The regulators consider that firms are not generally consumers and this applies to firms purchasing services from CTPs. As set out in the CBA, the regulators believe any indirect impact on the relevant markets or consumers is either mitigated or unlikely to be material. The regulators therefore consider the proposals to be compatible with the FCA's competition objective and duty.

FCA and PRA Secondary competitiveness and growth objective

11.12 As explained in the CBA, the regulators believe that the proposals will advance this objective. The proposals would increase the resilience of the financial sector as a result of more resilient third party services. This in turn will contribute to the making the UK financial system safe and attractive for business. While the proposals do impose new burdens, the CBA explains that third parties are likely to be subject to similar burdens in comparable regimes, especially the EU's DORA, and in many cases may already be preparing to meet such requirements. This will reduce the impact, while ensuring the wider benefits to the financial system contribute to the UK's continued position as an attractive place to do business.

Regulators' 'have regards' analysis

11.13 The following factors, to which all the regulators are required to have regard, were significant in their analysis of the proposal:

Efficient and economic use of regulator resources

- **Service-based approach:** the CP proposes a service-based approach to the oversight of CTPs. The proposals focus on the material services provided by CTPs to the financial sector. The measures would not involve regulators having wider responsibility for the supervision of CTPs as entities (as would be the case for a full supervisory regime for regulated firms) or the services they provide to other sectors. This approach is motivated in part by a concern for the efficient use of regulators' resources, as well as to reduce compliance costs for CTPs.

- **Leveraging external resources:** the regulators would consider taking into account testing undertaken by the CTPs themselves or by other (UK or overseas) authorities. Leveraging these external resources would help the regulators to use their resources efficiently and economically.
- **Efficient coordination between regulators:** by adopting a single unified policy and by issuing a joint CP, the three supervisory authorities will avoid the unnecessary duplication of efforts.

Proportionality

- **Focus on specific services:** By focusing the proposals primarily on CTPs' provision of material services to firms and FMIs, the regulators would ensure that restrictions imposed on CTPs are proportionate to the expected benefits – namely, management of the systemic risks to the regulators' objectives posed by third party service provision to the UK financial sector.
- **Responsibility lies with CTP:** The proposals would not impose new burdens or restrictions on firms and FMIs. The responsibility for satisfying the minimum resilience standards would rest with the CTP.
- **Principles- and outcomes-based approach:** rather than requiring CTPs to satisfy a checklist of controls, we propose that CTPs meet a principles-based set of minimum resilience standards.
- **Avoidance of unnecessary duplication:** the regulators have sought to minimise unnecessary duplication between the new CTP regime and existing certifications and standards. Similarly, by potentially taking into account resilience testing undertaken by CTPs themselves, other UK competent authorities or non-UK financial supervisory authorities, the regulators will minimise unnecessary duplication of testing. This avoidance of duplication will help to ensure that burdens and restrictions imposed by the regime are proportionate to its benefits.
- **Cost benefit analysis:** the regulators have also tested the proportionality of the costs imposed by the proposals in this CP as part of their cost benefit analysis.

Net Zero

11.14 The use of certain third-party services by firms and FMIs can offer improvements in energy efficiency that could beneficially affect their emissions profiles. By managing the systemic risks posed by third-party arrangements with CTPs, the policy proposals could give firms and FMIs greater confidence in the resilience of the relevant third-party services. It could be considered that the policy proposals might thereby indirectly facilitate the energy efficiencies these arrangements can offer by giving firms and FMIs

greater confidence to use such services. However, the regulators consider that any such effect would likely be small and indirect.

Consumers should take responsibility for their decisions

11.15 The regulators consider that the proposals will have a neutral impact on consumers' decision-making. The proposals are focused on CTPs providing services to firms and FMIs, and do not impact on firms providing services to consumers.

Responsibilities of senior management

11.16 The management body of an authorised firm or an FMI have a responsibility to maintain and enhance the firm's operational resilience. The regulators consider that the proposals in this CP, specifically the proposed governance requirement (Requirement 1) would support these responsibilities by requiring a CTP to:

- Appoint an employee or members of the governing body (who has appropriate authority, knowledge, skills, and experience) to act as the central point of contact for the regulators
- Establish clear roles and responsibilities at all levels of its staff involved in the delivery of any material services.
- Establish, oversee, and implement an effective approach that covers the CTP's ability to prevent, respond and adapt to, as well as recover from any event that disrupts the delivery of a material service, learn from those disruptive events and any testing of its material services undertaken.
- Ensure appropriate review and approval of any information provided to the regulators.

Desirability of publishing information

11.17 The regulators propose that a CTP would be required to prepare and share with those of their firm and FMI customers a summary report of assurance and testing activities carried out in compliance with the CTP regime. These proposals would ensure that relevant and actionable information about CTPs' compliance and risks is shared with their financial sector clients, while balancing the desirability of such information sharing with the need to protect the security of confidential and sensitive information.

Differences in the nature of business

11.18 With regard to firms and FMIs, the significance of the proposed CTP oversight regime derives from their increasing reliance on third-party services to support their operations. This reliance is a sector-wide trend that encompasses firms and FMIs with different business models and objectives. The regulators therefore regard the regime

as compatible with exercising its functions in a way that recognises differences in the nature, and objectives of businesses carried on by different firms and FMIs.

11.19 With regard to CTPs, the regime only applies when a prospective CTP has been assessed as providing services for which failure in, or disruption to, the provision of these services could threaten the stability of, or confidence in, the UK financial system. The regulators propose that all CTPs are therefore subject to consistent minimum requirements, expectations, and oversight. However, when overseeing CTPs, the regulators will take a proportionate approach, which may take into account the nature and objectives of the CTP's businesses. Moreover, the technology-neutrality of the proposed regime recognises differences in the in the business of CTPs.

Regulatory transparency

11.20 The regulators consider that the proposals in this CP accord with these principles of regulatory transparency. For example:

- **Discussion paper:** the regulators previously published DP3/22 – [Operational resilience: Critical third parties to the UK financial sector](#) to share and obtain views on potential measures to manage the systemic risks posed by certain third parties to the UK financial sector. The views obtained were taken into account in the development of the proposals in this CP.
- **Full consultation:** the regulators are publishing the present consultation to share their policy proposals with stakeholders and seek views.
- **Reasonable transparency on designation recommendations:** while the decision to designate a CTP rests with HMT, the regulators have been as transparent as reasonably possible regarding the kinds of factors they will consider when determining whether to recommend the designation of a provider. The desirability of transparency in this regard must be balanced against the need to allow for regulators' judgement and discretion in making a recommendation to HMT and the importance of making a holistic assessment of the systemic risk posed by a given provider.

Accountability and Consistency

11.21 The proposals in this CP accord with the principle of consistency in regulatory activities. They have been designed, where appropriate, to align with, and complement, existing regulatory obligations on firms and FMIs in relation to operational resilience and third-party risk management. The regulators will also set out, in a memorandum of understanding (MoU), how they will ensure coordination and consistency in the exercise of their respective function. HMT will lay this MoU before parliament, which will help uphold the regulators' accountability to the public and Parliament.

Supporting compliance and growth, and providing clear information, guidance and advice

11.22 In addition to proposed requirements in the Bank Rulebook, PRA Rulebook, and FCA Handbook, the regulators are proposing to publish a supervisory statement setting out their expectations of how CTPs should comply with and interpret the proposed requirements in their draft rules. The regulators also intend to publish a document setting out how they will carry out their oversight roles in relation to CTPs ('CTP approach document') in due course. The CTP approach document will help CTPs, firms, and FMIs understand how the regulators will oversee CTPs in practice and also uphold the regulators' accountability to the public and Parliament through greater transparency.

Impact on mutuals

11.23 The regulators consider that the impact of the proposed rule changes on mutuals is expected to be no different from the impact on other firms. The reason for this is that they are not proposing to place new obligations on any firms and FMIs.

FCA financial crime have regard

11.24 In formulating these proposals, the FCA has had regard 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). Financial crime is not the focus of this regime. However, the regulators do consider that the proposals will be neutral in respect of any risk under this have regard.

PRA Practitioner Panel

11.25 The PRA has consulted the Practitioner Panel, and taken account of its representations, as part of the process of developing the proposals in this CP.

FCA panel engagement

11.26 The FCA has consulted its Practitioner Panel, Listing Authority Advisory Panel, Consumer Panel, Small Business Panel, and Markets Panel in preparing these proposals, and has taken their feedback into account.

Economic growth under HMT remit letters

11.27 The PRA and FCA have had regard to medium to long-term economic growth as part of considering their secondary competitiveness and growth objectives, which requires the PRA and the FCA to act in a way that facilitates the growth of the UK

economy in the medium to long-term. As explained in the related analysis above, the regulators believe that the proposals in this CP may promote UK economic growth.

Competitiveness of UK economy

11.28 The PRA and FCA have had regard to the international competitiveness of the UK as part of considering the secondary competitiveness and growth objective. As explained in the analysis above, the regulators believe that the proposals in this CP are likely to promote the international competitiveness of the UK.

Equality and diversity

11.29 In making its rules and carrying out its policies, services, and functions, the regulators are required by the Equality Act 2010 to have due regard to the need to eliminate discrimination, to promote equality of opportunity, and to foster good relations between persons who share a protected characteristic and those who do not.

11.30 The regulators have considered the equality and diversity issues that may arise from the proposals in this consultation. The regulators do not consider that the proposals in this CP raise any concerns with regards to equality and diversity

Bank of England additional ‘have regards’ analysis

Effects of FMI functions

11.31 The Bank considers that the proposed CTP regime supports its financial stability objective by increasing the operational resilience of designated CTPs that offer services to firms or FMIs operating in another country, which can be argued as contributing positively to financial stability in that country. The regulators also note that the proposals allow for overseas entities to be designated as CTPs, and it can be argued that oversight of a designated CTP also enhances financial stability in other countries or territories which that CTP provides services to. Furthermore, the proposed oversight regime for CTPs has been designed to be as interoperable as reasonably practicable with similar regimes, such as the EU’s [DORA](#) and the US’s [BSCA](#).

Sustainable growth in the UK economy consistent with net zero and environmental targets

11.32 With respect to net zero and environmental targets, the Bank considers that the CTP policy proposals could accord with the need to contribute towards achieving compliance with the UK net zero emissions target, where the exercise of the Bank’s functions are relevant to the making of such a contribution. In particular, the Bank notes that the use of certain third-party services by firms and FMIs may offer improvements in energy efficiency that could beneficially affect their emissions profiles. The policy

proposals might facilitate this by giving firms and FMIs greater confidence to use such services, but the Bank considers that any such effect would likely be small and indirect.

11.33 With respect to sustainable medium or long-term growth in the UK economy, the Bank considers that the statement with respect to the PRA's and the FCA's secondary competitiveness and growth objectives and corresponding analysis in the CBA explains how the proposals in this CP are likely to promote UK economic growth.

Access to FMI services

11.34 The Bank of England does not consider that the proposals will affect the level of access to FMI services. The proposals do not place any requirements or expectations on FMIs themselves, or the entities that make use of FMIs' services (eg clearing members), and hence do not affect the accessibility of FMI services from a rules or expectations perspective.

12: Questions

1. Do you have any comments on the regulators' definitions of key terms and concepts outlined in Chapter 2 of the draft supervisory statement? Are there key terms or definitions the regulators could clarify or additional definitions to be included?
2. Do you have any comments on the regulators' overall approach to the oversight regime for CTPs outlined in Chapter 3 of the draft supervisory statement?
3. Do you have any comments on the regulators' proposed Fundamental Rules? Should the regulators add, clarify, or remove any of these Rules, or any of the terms used in them, eg 'prudent', 'responsibly'?
4. Do you have any comments on the regulators' proposal for the Fundamental Rules to apply to all services a CTP provides to firms or FMIs?
5. Do you have any comments on the regulators' proposed Operational Risk and Resilience Requirements? In particular, should the regulators add or remove any of these Requirements?
6. Are there any aspects of specific requirements that the regulators should clarify, elaborate on, or reconsider?
7. Do you have any comments on the regulators' proposal for the Operational Risk and Resilience Requirements to apply to a CTP's material services only?
8. Do you have any comments on the regulators' proposal to require CTPs to (separately) notify their firm/FMI customers and the regulators of relevant incidents?
9. Do you have any comments on the regulators' definition of 'relevant incident'?
10. Do you have any comments on the regulators' proposals to require CTPs to submit initial, intermediate, and final incident notifications to firms and FMIs and the regulators?
11. Do you have any comments on the regulators' proposals regarding what information should be included at each stage (initial, intermediate, or final) of notification?
12. What are your views on having a standardised incident notification template?
13. Do you have any comments on the regulators' proposed rules and expectations in relation to information gathering and testing?
14. What are your views on whether the regulators should include additional mandatory forms of regular testing for CTPs?
15. Do you have any comments on the regulators' proposals to require CTPs to share certain information with firms and FMIs?
16. Would the information the regulators propose to require CTPs to share benefit firms' and FMIs' own operational resilience and third-party risk management?

17. Do the regulators' proposals balance the advantages of sharing relevant information with firms and FMIs against potential confidentiality or sensitivity considerations for CTPs? Are there any additional safeguards that the regulators could consider to protect confidential or sensitive information?
18. Do you have any comments on the regulators' proposals to restrict CTPs from indicating, for marketing purposes, that designation implies regulatory endorsement or that its services are superior?
19. Do you anticipate any other unintended consequences from the designation of CTPs? Are any further requirements necessary to avoid these unintended consequences?
20. Do you have any comments on the cost-benefit analysis? Do you have any comments on the regulators' proposals to restrict CTPs from indicating for marketing purposes that designation implies regulatory endorsement or that its services are superior? Are there any other measures which the regulators could consider to mitigate potential, unintended adverse impacts on competition among third party service providers as a result of the designation of CTPs?