PS16/24 – Operational resilience: Critical third parties to the UK financial sector

PRA policy statement 16/24 | FCA policy statement 24/16

Published on 12 November 2024

Bank of England

FCA FINANCIAL CONDUCT AUTHORITY

Bank of England PRA

Content

1: Overview

1.1 This policy statement (PS) is issued jointly by the Bank of England (Bank), Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) (collectively 'the regulators'). It provides feedback to responses the regulators received to consultation paper (CP) 26/23 – **Operational resilience: Critical third parties to the UK financial sector**. It also contains the regulators' final policy, as follows:

- The regulators' final rules for critical third parties (CTPs) (hereafter 'the regulators' rules'), which are set out in the following rule instruments:
  - Bank of England FMI Rulebook: Critical third parties Instrument 2024 (Appendix 2);
  - Bank of England FMI Rulebook: Critical third parties Emergency Provisions Instrument 2024 (Appendix 2a);
  - PRA Rulebook: Critical third parties Instrument 2024 (Appendix 3);
  - FCA Handbook: Critical third parties Instrument 2024 (Appendix 4); and
  - FCA Handbook: Critical Third Parties Statement of Policy relating to Disciplinary Measures Instrument 2024 (Appendix 9)
- The regulators' joint final supervisory statement (SS) 6/24 – Operational resilience: Critical third parties to the UK financial sector (Appendix 5);
- The Bank/PRA's final SS 7/24 – Reports by skilled persons: Critical third parties (Appendix 6). The FCA's equivalent guidance on skilled persons reviews is in the FCA Handbook: Critical third parties Instrument 2024 (Appendix 4);
- The regulators' approach to the oversight of Critical third parties ('CTP approach document') (Appendix 7); and
- The Bank of England's approach to enforcement: proposed changes to statements of policy and procedure following the Financial Services and Markets Act 2023, (Appendix 8) which has also been published separately on the same date as this PS and should be read in conjunction with it, which contains the 'Bank's approach to enforcement in respect of critical third parties: statement of policy and procedure' (CTP Enforcement SoP). The FCA's equivalent and substantively identical approach to enforcement in respect of CTPs is in The FCA's Critical Third Parties Statement of Policy relating to Disciplinary Measures Instrument 2024 (Appendix 9).

1.2 Collectively, these documents are referred to as 'the CTP Oversight Regime'.

1.3 The overall objective of the final policy in this PS (hereafter the 'Overall Objective') is to manage 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 (either individually or, where more than one service is provided, taken together) that a CTP provides to one or more authorised persons, relevant service providers and/or financial market infrastructure entities (collectively 'firms').

1.4 This PS is primarily relevant to CTPs. As set out in s312L of FSMA[1] as amended by the FSMA 2023,[2] HM Treasury (HMT) may only designate a third party service provider as a CTP if, in its opinion, a failure in, or disruption to, the services that the third party provides to firms could threaten the stability of, or confidence in, the UK financial system. At the time of publication of this PS, HMT had not designated any CTPs. Guidance on HMT's approach to the designation of CTPs can be found in **Critical Third Parties – HM Treasury's Approach to Designation** Section 3 of the CTP approach document describes the regulators' approach to identifying potential CTPs to recommend to HMT for designation. The PS is also relevant to every 'Person Connected with a CTP',[3] including but not limited to undertakings in a CTP's group. Some of the regulators' statutory powers in relation to a CTP, such as the information-gathering power in s312P of FSMA, extend to Persons Connected to a CTP. In addition, some of the requirements in the regulators' rules, such as 'Operational Risk and Resilience Requirement 3: Dependency and supply chain risk management' may also be relevant to a CTP's interaction with Persons Connected to it (see paragraphs 2.91-2.95).

1.5 This PS is also relevant to firms. The CTP regime does not impose additional, explicit requirements or expectations on firms, but complements their existing requirements and expectations relating to operational resilience and third party risk management.[4] The regulators consider that the fact that a third party has been designated as a CTP by HMT does not mean that it is inherently more resilient or better suited to provide one or more services to a given firm than a non-designated third party providing the same or similar services. Once HMT designates a third party as a CTP, firms and (where applicable) their groups, will remain accountable and responsible for managing the risks in any outsourcing or third party arrangements they have, or may enter into, with that CTP (notwithstanding that some features of the CTP regime, such as the information-sharing requirements on CTPs, may assist firms in managing these risks).

Background

Legislative changes

1.6 FSMA 2023 amended FSMA to give HMT the power to designate certain third parties as CTPs, and the regulators powers to:

- make rules imposing duties on CTPs in connection with the services they provide to firms (s312M of FSMA) ('rulemaking powers');
- direct a CTP in writing to do anything or refrain from doing anything specified in the direction (s312N of FSMA) ('powers of direction');

- gather information from a CTP, and Persons Connected to a CTP, appoint or direct the appointment of skilled persons, and carry out investigations (s312P of FSMA) ('information-gathering and investigatory powers'); and
- take enforcement action against a CTP (s312Q and s312R of FSMA) ('disciplinary powers').

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

1.7 In CP26/23, the regulators proposed a range of requirements and expectations for CTPs, which were structured into the following chapters and divided into 20 questions:

- **Identifying potential CTPs and recommending them for designation (Chapter 2):** Chapter 2 of CP26/23 set out the regulators' thinking, at the time of publication of the CP, on how they may identify potential CTPs and recommend them to HMT for designation, including:
  - the criteria that the regulators proposed to use, which were based on the statutory test in s312L of FSMA that HMT must apply when it decides whether to designate a third party as a CTP; and
  - the sources of data and information that the regulators intended to use to inform their identification of potential CTPs.
- **Key terms (Chapter 3):** This chapter set out the key defined terms that the regulators proposed to use in their draft rules and the draft of SS6/24.
- **CTP Fundamental Rules (Chapter 4):** This chapter contained six proposed CTP Fundamental Rules that a CTP would be required to comply with in respect of all the services it provides to firms.
- **CTP Operational Risk and Resilience Requirements** (**Chapter 5):** This chapter set out eight proposed Operational Risk and Resilience Requirements that a CTP would be required to comply with in relation to the material services it provides to firms. The proposed CTP Operational Risk and Resilience Requirements covered:
  - Requirement 1: Governance;
  - Requirement 2: Risk management;
  - Requirement 3: Dependency and supply chain risk management;
  - Requirement 4: Technology and cyber resilience;
  - Requirement 5: Change management
  - Requirement 6: Mapping;
  - Requirement 7: Incident management; and
  - Requirement 8: Termination of services.

- **Information-gathering, testing, self-assessment and information sharing (Chapter 6):** This chapter included a range of proposed requirements relating to information-gathering, testing self-assessments and information-sharing for a CTP, including to:
  - submit self-assessments to the regulators within three months of designation, and annually thereafter;
  - regularly test its ability to continue providing material services in severe but plausible scenarios ('scenario testing');
  - annually test its financial sector incident management playbook jointly with an appropriately representative sample of the firms it provides services to;
  - share certain information with the firms it provides services to (including a summary of its self-assessments); and
  - meet the requirements on skilled person reviews, and the accompanying expectations in the draft of SS7/24.
- **Notifications (Chapter 7)**: This chapter contained proposed requirements for a CTP to notify certain incidents to the regulators, and to the firms to which they provide the impacted service(s). The chapter proposed a phased approach to these incident notifications and set out the information that a CTP would be required to provide in each phase.
- **Referrals to oversight by the regulators (Chapter 8):** This chapter contained proposed requirements that a CTP, and persons acting on their behalf, would have to comply with when publicly referring to the fact that it was designated as a CTP by HMT, and overseen by the regulators.
- **Designation and nomination of a legal person in the UK and emergency relief (Chapter 9):** This chapter included:
- proposed requirements for a CTP without a UK head office, branch or subsidiary ('establishment) to nominate a legal person to perform certain functions on its behalf (such as receiving statutory notices under FSMA); and
- proposed requirements for a CTP relating to record keeping, and the Bank's proposals to provide regulatory relief to a CTP in emergency circumstances (the equivalent PRA and FCA provisions are set out in the **PRA Rulebook** and **FCA Handbook** respectively will also apply to CTPs automatically).

1.8 In determining their policy, the regulators considered representations received in response to CP26/23. In this PS, the 'Summary of responses' contains a general account of the representations made in response to the CP and the 'Feedback to responses' chapter contains the regulators' feedback. Details of any changes of note relative to the proposals consulted on are also covered in this document.

1.9 In carrying out their respective policy making functions, the regulators are required to have regard to various matters. In CP26/23 the regulators explained how they had regard to the most relevant of these matters in relation to the proposed policy. The 'Changes to draft policy' section of this chapter refers to that explanation, taking into account consultation responses where relevant.

Summary of responses

1.10 The regulators received 62 responses to CP26/23 from third party service providers, firms, FMIs, trade associations representing the financial services and technology sectors, consultancy firms and law firms. Appendix 1 lists the respondents to the CP who consented to their names being published or subsequently made public the fact that they had responded to the consultation.

1.11 Respondents generally supported the Overall Objective and the regulators' proposed approach. However, they requested changes and clarifications to various aspects of the proposals, which Chapter 2 of this PS examines in detail.

1.12 Feedback from third party service providers and firms often diverged, which is in itself significant as it provided a broad spectrum of views. The former were keen to minimise the potential compliance costs of the proposed CTP oversight regime by encouraging the regulators to rely as much as possible on CTPs' existing assurance mechanisms, recognised industry certifications, internal processes and testing etc. The latter wanted greater accountability and information-sharing from the CTPs they receive services from.

Changes to draft policy

1.13 Where the final rules differ from the draft in the CP in a way which is, in the opinion of the regulators, significant, FSMA[5] requires the regulators to publish:

- details of the differences together with an updated cost benefit analysis; and
- a statement setting out in the regulators' opinion whether or not the impact of the final rules on mutuals is significantly different from: the impact that the draft rules would have had on mutuals; or the impact that the final rules will have on other firms.

1.14 While the regulators do not consider that the changes in the final rules are significant, in response to feedback to CP26/23 the regulators have made the following changes of note:

- provided additional guidance in the CTP approach document on their approach to identifying potential CTPs and recommending them for designation to HMT;
- added a new section to SS6/24 explaining how the disruption or failure of a CTP's services to firms could impact the stability of, or confidence in, the UK financial system. The new section builds on the analysis in the **Macroprudential approach to operational resilience** published by the Bank's Financial Policy Committee (FPC);

- added, amended, clarified and/or deleted several key defined terms in their rules and SS6/24, including but not limited to renaming ‘material services’ ‘systemic third party services’ to better reflect the systemic risk posed by the potential disruption or failure of these services;[6]
- recognised the ‘shared responsibility model’ in SS6/24 (defined in section 2 of SS6/24) while explaining its limitations when it comes to managing systemic risk;
- limited the scope of CTP Fundamental Rules 1-5 to a CTP’s provision of ‘systemic third party services’ to firms. CTP Fundamental Rule 6 will continue to apply in relation to all the services that a CTP provides to firms;
- clarified in SS6/24, including through non-exhaustive examples, how a CTP should interpret and comply with certain requirements in the CTP Fundamental Rules, such as ‘acting in a prudent manner’, and ‘disclosing to the regulator appropriately anything relating to the CTP of which they would reasonably expect notice’;
- amended and clarified various aspects of the CTP Operational Risk and Resilience Requirements in the rules and SS6/24, including but not limited to:
    - making ‘Requirement 3: Dependency and supply chain risk management’ more proportionate including by limiting the most onerous requirements it imposes on a CTP to its ‘Key Nth Party providers’ (ie persons that are part of a critical third party’s supply chain and are essential to the delivery of a systemic third party service to one or more firms) and ‘Persons Connected to a CTP’, while continuing to ensure that CTPs adequately consider all risk to their supply chain;
    - amended and clarified aspects of ‘Requirement 7: Incident Management’. In particular, by:
        - removing the expectation on a CTP in the draft of SS6/24 to ‘take into account and (to the extent possible) be compatible with the impact tolerances that firms have set for any important business services that are supported by the material service’ when complying with the requirement to set an ‘appropriate maximum tolerable level of disruption’ for each systemic third party services it provides to firms (and providing additional guidance on how a CTP should approach this requirements);
        - allowing a CTP to use its existing, documented incident management policies and procedures instead of developing a bespoke ‘financial sector incident management playbook’ for its UK firm customers, as long as these policies and procedures meet the outcomes specified in the regulators’ rules and SS6/24; and
- amended the requirements on assurance, information-sharing and self-assessment for CTPs to:
    - distinguish:

    - the self-assessment that a CTP must provide to the regulators within three months of designation (renamed ‘interim self-assessment’); from
    - the self-assessment that it must provide to the regulators and the firms it provides systemic third party services to annually thereafter (‘annual self-assessment’);
- clarified in SS6/24 the regulators’ expectations of how CTPs should comply with the requirements on:
    - scenario-testing; and
    - incident management playbook exercises (as renamed)’
- amended the incident notification (renamed ‘incident reporting’) requirements for CTPs, including by:
    - reviewing the proposed definition of a ‘relevant incident’ (renamed ‘CTP operational incident’); and
    - clarifying and streamlining the information that CTPs will be required to provide in their initial, intermediate and final incident reports; and
- replaced the proposed requirement to nominate a UK legal person for a CTP without a UK establishment, with a simpler requirement for all CTPs to provide an address for service in the UK.

1.15 The regulators view these changes as beneficial because they make the requirements for CTPs in their final rules, and the accompanying expectations in SS6/24:

- clearer and easier for CTPs to interpret, understand and implement;
- more consistent with the Overall Objective; and
- more proportionate, resource-efficient, and risk-based.

1.16 The final policy and rules in this PS have also been informed by recent lessons learnt from operational incidents at third party service providers to the financial sector and other sectors. As noted in the FCA’s recent note on **lessons learnt** from the CrowdStrike outage, ‘since the beginning of 2023, we’ve seen a continued trend of third-party related incidents’. Between 2022-2023 third party related issues were the leading cause of operational incidents reported to the FCA. While every incident is unique, there are evident recurrent themes, which the policy in this PS seeks to address. For instance, the importance of CTPs:

- managing risks in their supply chain;
- taking reasonable steps to ensure the adequacy of IT products and services, including updates thereto, before releasing them to firms; and
- providing accurate, clear, effective and timely information and support to the regulators, and affected firms (individually and collectively) during incidents.

1.17 When making rules, the regulators are required to comply with several legal obligations. At the consultation stage, in **CP26/23** the regulators published an explanation of their reasons for believing that making the proposed rules are compatible with their objectives, the regulatory principles,[7] and other duties.[8] The regulators, having considered responses to CP26/23 and, in light of the changes the regulators have made to the policy, consider that the assessment in CP26/23 applies also to the final rules and policy as set out in this PS. In making changes since the consultation stage, the regulators have considered their statutory obligations and their duties to have regard to the regulatory principles. The regulators consider that, following the changes to the policy, there are, in some cases, additional reasons to expect the policy to accord with these obligations. For example, some of the changes enhance the proportionality of the policy, in line with the regulatory principles.

1.18 Since the final rules apply only to CTPs, the impact of the final rules on mutuals is not significantly different from the impact that the draft rules would have had on mutuals or the impact that the final rules will have on other firms.

1.19 The changes we have made to our rules and guidance do not significantly change our cost benefit analysis (CBA). In this PS we discuss the changes to the policy and outline the impacts on the CBA.

Format of the regulators' draft rules

1.20 Each regulator has different statutory objectives and an individual statutory power to make rules for CTPs. However, the Overall Objective is common to all three regulators. The regulators also have a statutory duty to coordinate the exercise of their oversight functions over CTPs (s312U of FSMA), including their respective rulemaking powers.

1.21 As a result, the requirements for CTPs in the regulators' rules are set out in three separate rule instruments, one issued by each regulator. These three rule instruments are identical in effect and substance and should be interpreted accordingly.

1.22 Each regulator will apply its instruments to every CTP designated by HMT, regardless of the firms to which the CTP provides services. Consequently, a CTP should be able to pick up any of the regulators' rule instruments and understand all the requirements it is subject to. References to the 'regulators' rules' in this PS and the SS6/24 should be interpreted as encompassing all three rule instruments.

1.23 To further facilitate a CTP's understanding of, and compliance with, the regulators' rules, SS6/24 has been issued jointly by the regulators and should be the main source of guidance for CTPs on how the regulators expect them to interpret and comply with the requirements in

their rules. At the start of each chapter and, where appropriate, other sections of SS6/24, the regulators have highlighted where the relevant requirements are found in each of their respective rule instruments.

1.24 As required by s312V of FSMA, HMT has laid before Parliament the regulators' **Memorandum of Understanding** (MoU) describing how they intend to coordinate the exercise of their respective functions in respect of CTPs.

Implementation

1.25 The final rules for CTPs will take effect from 1 January 2025. However, the statutory obligations of a CTP under FSMA, the requirements in the regulators' rules and the expectations in the SS6/24 and other documents listed in this PS, will only apply to a CTP on the date the designation order made by HMT comes into force. In addition, compliance with certain requirements in the regulators' rules will be subject to a transitional period that will also start from the date specified by HMT in the designation order. Chapter 2 of this PS and Section 12 of SS6/24 list the requirements that are subject to a transitional period and the applicable transitional periods.

2: Feedback to responses

2.1 Before making any proposed rules, the regulators are required by FSMA to have regard to any representations made to them in response to the consultation, and to publish an account, in general terms, of those representations and its feedback to them.[9]

2.2 The regulators have considered the representations received in response to the CP26/23. This chapter sets out their feedback to those responses, and their final decisions.

2.3 The sections below have been structured broadly along the same lines as the chapters of the CP, with some areas rearranged to better respond to related issues. The responses have been grouped as follows:

- Identifying potential CTPs and recommending them for designation;
- Key Terms;
- Overview of the oversight regime for CTPs;
- CTP Fundamental Rules;
- CTP Operational Risk and Resilience Requirements;
- Self-assessment, scenario tests, incident management playbook exercises and information sharing;
- Incident reporting and other notifications;
- Competition and unintended consequences
- UK address for services; and

- Cost benefit analysis.

Identifying potential CTPs and recommending them to HMT for designation

2.4 In section 2 of CP26/23, the regulators set out their thinking, at the time of publication of the CP, on how they would identify potential CTPs and recommend them to HMT for designation, including:

- the criteria that the regulators intended to consider; and
- the sources of data and information they would use.

2.5 Several respondents asked for additional guidance on how the regulators would identify potential CTPs and recommend them for designation to HMT. In particular:

- how the regulators would assess the materiality of a CTP's services from a systemic risk point of view, and how this assessment would differ from how individual firms assess the materiality of their outsourcing and third party arrangements;
- the sources of data and information that the regulators would consider;
- clarification that the regulators would not recommend for designation:
  - intra-group service providers; and
  - firms in respect of services provided to other firms where those services are already subject to regulation and supervision by one or more regulators (eg custody, clearing etc.); and
- how the designation process would work in practice, including the anticipated level of engagement between a potential CTP, HMT and the regulators.

2.6 In response to feedback, the regulators have taken the text in Chapter 2 of CP26/23, provided additional guidance on the areas identified by respondents, and included it in chapter 3 of the CTP approach document. The regulators' approach to identifying potential CTPs and recommending them for designation to HMT will evolve over time, and this chapter will therefore be updated as appropriate.

2.7 In March 2024, HMT published **Critical Third Parties – HM Treasury's Approach to Designation** which outlines its envisaged end-to-end process for designating a CTP from initial receipt of a recommendation by the regulators, to publication of the designation order. A potential CTP should read chapter 3 of the CTP approach document in conjunction with HMT's 'Approach to Designation' document as it will be HMT that ultimately makes the final decision as to that potential CTP's designation.

Key terms

2.8 In CP26/23, the regulators proposed a set of key defined terms to facilitate a clear and consistent understanding of the proposed requirements for CTP in their draft rules, and the accompanying expectations in the draft supervisory statement.

2.9 Respondents welcomed the proposed inclusion of key defined terms and the approach of adopting existing, internationally recognised, key defined terms (such as those in the Financial Stability Board's (FSB) **Cyber Lexicon** where possible. However, they also suggested amendments and clarifications to several key defined terms.

2.10 In response to feedback, the regulators have made changes to various key defined terms. These changes are summarised in paragraphs 2.11 – 2.23 below (except for the amended definition of 'relevant incident,' which has been renamed 'CTP Operational Incident', and is examined in the section on 'Incident reporting, and other notifications' below).

Material service

2.11 Two respondents suggested that the term 'material service' be replaced with an alternative term that reflected more accurately the potential systemic risk posed by the failure in, or disruption to this subset of services that CTPs provide to firms. For instance, 'systemic third party service' or 'systemic service'. One of these respondents noted that 'material outsourcing' was already a defined term in the **PRA's** and **FCA's** rules on outsourcing and third party risk management for firms, and argued that the additional use of the term 'material service' in the CTP oversight regime could create confusion.

2.12 Two respondents suggested that the definition of 'material service' should explicitly reference firms' important business services (IBSs) (as defined in the regulators' respective **operational resilience** rules, accompanying expectations and guidance for firms) since the systemic materiality of a CTP's service would depend (in part) on the IBSs whose delivery it supported in the CTP's customer firms.

2.13 One respondent argued that the reference to 'confidence in the UK financial system' should be deleted as it made the proposed definition of 'material service' too subjective. Another respondent highlighted more generally that the notion of confidence was not universally understood and had no commonly agreed measure.

2.14 After considering these responses, the regulators have:

- replaced the key defined term 'material service' with 'systemic third party service' in their final rules, SS6/24 and other relevant documents to promote clarity by better reflecting the potential systemic risk posed by the disruption or failure of these services;

- adopted the definition of ‘service in s312(8)L of FSMA in their rules, and clarified in SS6/24 that ‘service’ should be interpreted as including:
  - ‘third party service relationships’ as defined in the FSB **Final report on enhancing third party risk management and oversight – a toolkit for financial institutions and financial authorities** FSB TPR Toolkit); and
  - Information and communication technology (ICT) services.

2.15 The regulators have decided not to refer explicitly to IBSs in the definition of a systemic third party service. As discussed in the previous section, and in chapter 3 of the CTP approach document, when identifying potential CTPs and the systemic third party services they provide to firms, regulators will consider several criteria and draw upon a number of sources of data and information, including but not limited to the IBSs whose delivery these third party service support (as reported by firms in the outsourcing and third party (OATP) register). Moreover, the fact that a service provided by a third party service provider supports the delivery of one or more IBSs at one firm will not necessarily or automatically make this service a potential systemic third party service. The regulators’ identification of systemic third party services will include additional considerations. Explicitly referring to IBSs in the definition of a ‘systemic third party service’ would therefore provide an incomplete and misleading articulation of why the regulators consider that the disruption or failure of these services could pose risks to the stability of, or confidence in, the UK financial system.

2.16 The regulators have kept the reference to ‘confidence in the UK financial system’ in the definition of a ‘systemic third party service’. The statutory test for designation of a third party as a CTP by HMT (s312L of FSMA) explicitly mentions the potential for the failure or disruption of a CTP’s services to impact the stability of, **or confidence in**, the financial system (emphasis added). It is therefore congruent to also mention confidence in the definition of a systemic third party service in the regulators’ rules. Moreover, the FPC’s macroprudential approach to operational resilience and section 3 of SS6/24 both note that a ‘loss of confidence is the transmission channel by which an operational incident [including at a CTP] may most likely lead to financial instability,’ even if loss of confidence is harder to measure than other channels that could lead to the transmission of an operational incident across the financial system, such as operational and financial contagion.

Disruption

2.17 Several respondents asked for greater clarity on the proposed definition of ‘disruption’ in CP26/23. One respondent commented that the proposed definition was too broad as it would apply in relation to all the services that a CTP provides to firms, and suggested that it should only apply in relation to a CTP’s provision of systemic third party services to firms.

2.18 In response to this feedback, the regulators have revised the definition of ‘disruption’ so that it only applies in relation to a CTP’s provision of systemic third party services to firms. This aligns to the scope of application of most of the regulators’ rules that impose significant substantive obligations on CTPs, and makes the regime more proportionate.

Vulnerability

2.19 Four respondents expressed concern about the use of the term ‘vulnerability’ in various parts of the draft rules and the draft supervisory statement. These respondents explained that, in cyber-security terminology, the term ‘vulnerability’ would be defined as ‘a weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats’. However, in various parts of the regulators’ draft rules and draft supervisory statement, ‘vulnerability’ was used in a general, ordinary-language sense. Respondents were particularly concerned about potential requirements or expectations on CTPs to disclose unremedied vulnerabilities (in the cyber-security sense) to the regulators and to the firms they provide systemic third party services, as this could increase the risk of threat actors exploiting these vulnerabilities, which would go against the Overall Objective. Two respondents suggested alternative terms that could replace ‘vulnerability’ to avoid potential ambiguity or misunderstandings: ‘material area for improvement’ or ‘resilience vulnerability,’

2.20 In response to this feedback, the regulators have:

- reviewed all uses of the term ‘vulnerability’ in their rules (where it is now only mentioned once) and, in particular, SS6/24;
- replaced all instances where ‘vulnerability’ was used in its ordinary-language meaning with ‘areas of improvement’; and
- removed any requirements and expectations on CTPs to disclose unremedied vulnerabilities (in the cyber-security sense) to the regulators and to the firms they provide systemic third party services to.

2.21 There are two instances in the SS6/24, where the term ‘vulnerability’, in the cyber-security sense, is intentionally used:

- in section 6, which notes that, as part of its compliance with Operational Risk and Resilience Requirement 5, which deals with a CTP’s technology and cyber resilience; a CTP should have ‘capabilities to identify, assess and promptly remediate vulnerabilities relating to information and technology assets’; and
- in section 8, which deals with incident reporting, and explains an example of the type of information that may assist the regulators and affected firms in understanding the nature and extent of the CTP operational incident ‘whether the attack involved the exploitation of vulnerabilities listed in a public Common Vulnerabilities and Exposures database’.

2.22 In addition, section 3 of the SS6/24 uses the term ‘macro vulnerability’ as described in the FPC’s **macroprudential approach to operational resilience** and clarifies how it should be interpreted.

Shared responsibility model

2.23 One respondent asked for the ‘shared responsibility model’ to be added to the list of key defined terms. The regulators have done so and provided guidance on the shared responsibility model, and its limitations when it comes to managing systemic risk, in SS6/24 (see next section).

Overview of the oversight regime for CTPs

2.24 In section 3 of the draft supervisory statement – Operational resilience: Critical third parties to the UK financial sector, the regulators outlined their overall approach to the oversight regime for CTPs. This section covered the following areas:

- Overall Objective;
- Focus on CTPs’ services to firms;
- Interaction with the requirements for firms;
- The shared responsibility model;
- Alignment to international standards;
- Proportionality;
- Format of the regulators’ rules for CTPs;
- SS6/24;
- The Bank of England’s Statement of Policy and Procedures related to enforcement on CTPs and the FCA Handbook: Critical third parties (Statement of Policy) relating to Disciplinary Measures Instrument 2024; and
- Transitional arrangements.

Overall objective of the CTP oversight regime

2.25 Most respondents supported the Overall Objective and welcomed the regulators’ proposed approach to delivering it, which they described as proportionate, reasonable, and robust. One respondent argued that it was vital that CTPs are subject to appropriate regulation and oversight to manage potential systemic risk. Only one respondent challenged the Overall Objective arguing that there was no evidence that improving the resilience of CTPs was required. The same respondent also expressed doubts as to what oversight of CTPs would entail, and the regulators’ competency to provide such oversight.

2.26 Most respondents welcomed the proposed CTP oversight regime’s principles-based, outcomes-focused, and technology-neutral approach. Some respondents noted that this approach should be flexible enough to accommodate the operating models of different types

of CTP, such as those that provide services to customers in other jurisdictions and to other industry sectors in addition to financial services.

New section in the SS6/24 on how CTPs could impact the stability of, or confidence in, the financial system

2.27 Notwithstanding the overall support for the proposed CTP oversight regime, responses from third party service providers revealed gaps in their understanding of how disruption to their services (if they were to be designated as CTPs) could impact the stability of, or confidence in, the UK financial system. These knowledge gaps are understandable at this stage, as potential future CTPs may not:

- understand how the financial system works and the interconnections between firms and other market participants;
- know how their customer firms configure and use their services or the extent to which these services support these firms' delivery of IBSs;
- have experience being directly regulated and overseen. In particular, by financial regulators; or
- consider systemic risk when designing and delivering their services.

2.28 Although understandable, these knowledge gaps are an obstacle to the effective implementation of the CTP oversight regime, as they may result in some CTPs:

- complying with the letter but not the spirit of the regulators' rules, and the accompanying expectations in SS6/24;
- not fully understanding the rationale for and the importance of certain requirements in the regulators' rules, such as those on incident management and incident reporting; and
- unduly seeking to minimise the compliance costs of the CTP oversight regime by expecting the regulators to rely solely on certain existing forms of assurance (eg recognised certifications) without first considering whether these forms of assurance are adequate to manage the systemic risks that CTPs pose to the financial system.

2.29 In March 2024, the Bank's FPC published its macroprudential approach to operational resilience. This publication illustrated how the resilience of individual firms, while providing the essential foundation for operational resilience across the UK's financial system, may not, by itself, be sufficient to ensure system-wide resilience. The FPC's macroprudential approach to operational resilience identified additional 'macro vulnerabilities' in the financial system, including the financial sector's increasing reliance on certain services provided by third party service providers.

2.30 To clarify and illustrate the systemic risks posed by the potential failure in, or disruption to a CTPs' services to firms (and address the knowledge gaps observed in responses to the CP), the regulators have included a new section in SS6/24 (section 3), which applies the analysis in the FPC's macroprudential approach to operational resilience to CTPs. This section puts the regulators' requirements and expectations for CTPs in the context of the systemic risks that they seek to manage. By doing so, it seeks to bridge the knowledge gap described above.

Proportionality

2.31 Most respondents emphasised the need for proportionality in the requirements and expectations for CTPs, and in the regulators' implementation of the CTP oversight regime. Respondents noted that proportionality would allow CTPs with varied sizes and business models to compete on an equal footing and mitigate the risk of potential unintended consequences, such as stifling innovation.

2.32 Respondents urged the regulators to:

- consider the nature and operating model of different CTPs in their rules and accompanying expectations in SS6/24;
- avoid duplication between these rules and expectations, and existing requirements applicable to CTPs; and
- consider the compliance challenges that CTPs will face initially and implement the CTP oversight regime progressively.

2.33 The regulators have considered these points and embedded them throughout their rules, SS6/24 and CTP approach document.

Focus on CTPs' services to firms

2.34 Most respondents welcomed the CTP oversight regime's focus on the services that CTPs provide to firms, but raised questions about how this would work in practice.

2.35 Respondents had mixed views on the proposed scope of application of the regulators' rules. Most respondents agreed that the regulators' rules for CTPs, and accompanying expectations in SS6/24, should apply only in relation to a CTP's provision of systemic third party services to firms, as this would be more consistent with the Overall Objective, and more proportionate.

2.36 However, two respondents noted that:

- there may be risks to a CTP besides those relating directly to its delivery of systemic third party services, which should not be overlooked. For instance, risks to its financial

resilience; and
- limiting the scope of the regulators' rules only to systemic third party services may not guard against future threats. This respondent suggested an alternative tiered approach where all CTPs would be required to meet the Operational Risk and Resilience Requirements at progressively advanced levels relative to the systemic importance of each of their services.

2.37 Relatedly, several respondents asked for clarity (including examples) in respect of the circumstances in which the regulators may look at the non-systemic third party services that a CTP provides to firms. One respondent suggested that non-systemic third party services should only be looked at if they support the end-to-end delivery of a systemic third party service.

2.38 In response to this feedback, the regulators have:

- limited the scope of all Fundamental Rules imposing substantive obligations on a CTP, except CTP Fundamental Rule 6, to a CTPs' provision of systemic third party services to firms (see next section);
- clarified that a group of connected services may be treated as a single systemic third party service if these services are connected in such a way that the disruption or failure of one service could cause the disruption or failure of one, more or all of the services to which it is connected; and
- clarified that, consistent with the Overall Objective, a CTP should treat anything that could reasonably impact the resilience of a systemic third party service as being in scope of the CTP oversight regime. SS6/24 includes non-exhaustive examples of areas that could reasonably impact the resilience of a systemic third party service.

2.39 The tiered approach suggested by one respondent would be unduly complicated to oversee in practice across all CTPs and the services they provide. However, the regulators have clarified in SS6/24 that a CTP should ensure that all its services to firms meet appropriate levels of resilience that reflect their relative importance and risk profile. The regulators have also noted in SS6/24 that a CTP may voluntarily apply the requirements in their rules, and the expectations in SS6/24 to some or all its non-systemic third party services as best practice.

Interaction with the requirements for firms

2.40 Respondents understood, acknowledged and welcomed the fact that the oversight regime for CTPs will: (i) complement the requirements and expectations for firms relating to operational resilience, and outsourcing and third party risk management; but (ii) will not eliminate or reduce the accountability and responsibility of firms, their boards and senior

management (including, where applicable, individuals performing Senior Management Functions (SMFs) under the Senior Managers & Certification Regime) for meeting applicable requirements.

2.41 Some respondents asked how the CTP regime would operate alongside firms' existing obligations in practice. One respondent noted that the oversight regime could indirectly create additional obligations for firms in practice. For instance, a CTP could request information from its customer firms to respond to an information request from the regulators, which those firms had already provided to the regulators directly, leading to duplication. Another respondent asked:

- whether a firm could continue using a systemic third party service provided by a CTP if the regulators found significant failings in that service; and
- at what point this firm could be satisfied that these failings had been or would be addressed.

2.42 As stated in CP26/23, the accountability and responsibility of individual firms, their boards and senior management relating to operational resilience, and outsourcing and third party risk management will not change due to the implementation of the CTP oversight regime.

2.43 However, the information that CTPs will, under the regime, be required to share with the firms to which they provide systemic third party services should enable those firms to discharge their responsibilities in a more efficient and informed manner. If the regulators discover a significant failing in one or more of a CTP's systemic third party services and firms which receive those services are made aware of this failing, these firms will remain responsible for deciding what actions to take to mitigate the risks that the identified failing may pose to their operational resilience. The only exception would be if the regulators use their disciplinary powers under s312R of FSMA to impose conditions, limitations, prohibitions or restrictions (see the CTP enforcement SoP).[10]

The shared responsibility model

2.44 Several respondents recommended that, in addition to including the 'shared responsibility model' as a defined term, the regulators' rules and expectations for CTPs should take the shared responsibility model into account to reflect the allocation of security and resiliency responsibilities between a CTP and the firms it provides systemic third party services to. These respondents pointed out that the PRA already recognised the shared responsibility model in SS2/21 – **Outsourcing and third party risk management**.

2.45 In response to this feedback, the regulators have noted in SS6/24 that:

- a CTP's duties under the CTP oversight regime should generally align to its areas of responsibility under the shared responsibility model;
- CTPs are not required or expected to assume responsibilities that clearly fall to their customer firms; and
- during a CTP Operational Incident, it is likely that both CTPs and affected firms will need to take a combination of individual, collective and collaborative response and recovery measures in line with their respective regulatory obligations.

2.46 However, the regulators have also explained in SS6/24 that, while the shared responsibility model can be relevant to the demarcation of a CTP's duties under the CTP oversight regime, the model is not designed with systemic risk in mind. The shared responsibility model sets out the respective responsibilities of two parties to a transaction but, in doing so, does not consider the cumulative impact that the disruption or failure of the services that one party (the CTP) provides to multiple firms (which may in turn be interconnected) may cause. The fact that the shared responsibility model does not recognise the asymmetric impact of a CTP not meeting its responsibilities relative to the impact of an individual firm not doing so, inherently limits its applicability as a tool for managing systemic risks. The requirements in the regulators' rules, and the accompanying expectations in SS6/24 seek to address these inherent gaps in the shared responsibility model when it comes to systemic risk.

Alignment to international standards and interoperability with non-UK regimes

2.47 One of the points that respondents raised most frequently and strongly was the importance of the CTP oversight regime aligning to international standards and being interoperable with similar non-UK regimes, such as the oversight regime for critical information and communications technology (ICT) service providers under the EU's **Digital Operational Resilience Act** (DORA). One respondent noted that regulatory consistency and coordination within the financial sector and with other authorities that have remit over potential future CTPs would be essential to make the CTP oversight regime successful.

2.48 Most respondents complimented the regulators' efforts to leverage global standards, such as Basel Committee's **Principles for operational resilience** and the **FSB TPR Toolkit** in their proposals for CTPs. Respondents also welcomed the regulators' commitment to promoting interoperability with regimes such as DORA.

2.49 In parallel to developing and implementing the oversight regime for CTPs, the regulators are continuing their dialogue with international counterparts to strengthen bilateral and multilateral cooperation in this area.

2.50 Two respondents raised concerns regarding the regulators' proposal to request information that a CTP had provided to non-UK authorities if relevant to the oversight regime for CTPs. These concerns did not accord with feedback from the same respondents emphasising the importance of cross-border regulatory and supervisory coordination as a way of minimising duplicative oversight of, and information requests to, CTPs. To address these concerns, these respondents suggested that regulators' requests for information that a CTP had provided to other authorities should be directed to those authorities rather than the CTP, or alternatively, if these requests were addressed directly to the CTP:

- they should be explicitly tied to an identifiable requirement under the CTP oversight regime or a list the information that the regulators can request should be included in SS6/24;
- the CTP should not have to disclose to the regulators' information provided to other authorities unless those authorities carry out similar functions to or have overlapping mandates with the regulators, the information requested has an actual nexus to the services the CTP provides to UK firms and the other authorities' consent to be shared;
- the regulators' information requests should consider any prohibitions on disclosure that CTPs might be subject to, including obligations owed to customers - especially customers which are not UK firms; and
- the regulators should provide assurance that they will exercise their information-gathering powers proportionately to obtain information relating to the risks they seek to mitigate, including by requesting the minimum amount of information to achieve their purpose, and ensuring appropriate safeguards are in place to protect the information they request.

2.51 The regulators recognise the need for proportionality when requesting information from a CTP that it has provided to other authorities. However, some of the suggestions referred to above would unduly constrain the regulators' discretion to exercise their statutory information-gathering powers under s312P of FSMA to request any 'information and documents reasonably required in connection with the exercise of their functions conferred on it by or under' FSMA. The regulators have recognised in the CTP approach document that there may be legal restrictions on the ability of CTPs to share information provided to other authorities. Consequently, the regulators may seek this information directly from relevant authorities (either alternatively or in addition to requesting it from CTPs) if there are appropriate:

- cooperation arrangements in place eg Memoranda of Understanding (MoUs);
- information-sharing gateways; or
- multilateral fora where authorities can share this information, such as supervisory colleges.

Transitional arrangements

2.52 Several respondents emphasised the need for an appropriate transitional period (starting on the date specified by HMT in the designation regulations) for a CTP to comply with the requirements in the regulators' rules, and the accompanying expectations in SS6/24. One respondent encouraged the regulators to provide at least a 12 month implementation period from the date of a CTP's designation for all requirements, and consider further extensions/flexibility for more complex requirements.

2.53 The regulators recognise that some requirements in their rules will require new or enhanced processes at a CTP, which justify a transitional period. Section 12 of SS6/24 lists those requirements that are subject to a transitional period.

2.54 The CTP approach document further clarifies that the regulators' interaction with a CTP in the first year following its designation will differ from their subsequent, business-as-usual oversight, and will focus on helping the regulators better understand the CTP with the objective of forming an initial view of the key risks it poses to their objectives.

2.55 Although the requirements in the regulators' rules apply directly to CTPs they may, in practice, require amendments to their contractual arrangements with firms and their Key Nth party providers. Where this is the case, SS6/24 notes that a CTP should seek to review and update contractual agreements pre-dating its designation at the first appropriate contractual renewal or revision point following their designation.

CTP Fundamental Rules

2.56 In Chapter 4 of CP26/23, the regulators proposed six Fundamental Rules that CTPs would be required to comply with in respect of all the services that they provide to firms. Modelled broadly on the PRA's Fundamental Rules and the FCA's Principles for Business which apply to firms, these high-level rules articulate fundamental behaviours that the regulators require of CTPs given the Overall Objective.

2.57 Thirty-eight respondents expressed support for the proposed CTP Fundamental rules. One respondent welcomed the proposed rules as a high-level base of expectations for CTPs. Two other respondents encouraged aligning the proposed Fundamental Rules with the PRA Fundamental Rules, and FCA Principles for the Business.

2.58 Two respondents opposed the introduction of the Fundamental Rules for CTPs. One of these respondents challenged the need for the CTP Fundamental Rules and argued that the Overall Objective could be delivered via the eight Operational Risk and Resilience Requirements (see section 'CTP Operational Risk and Resilience Requirements'). The second respondent regarded the CTP Fundamental Rules as redundant given that corporate law contains similar requirements.

2.59 The regulators do not agree with the proposals to remove the CTP Fundamental rules, as doing so would significantly undermine the enforceability and effectiveness of the CTP oversight regime. While the behaviours that the CTP Fundamental Rules require align to existing legal requirements that apply to some CTPs under the corporate law of the UK or other jurisdictions, and/or may be reflected in their by-laws this does not eliminate the need for the CTP Fundamental Rules.

2.60 Notwithstanding the broad support for the introduction of the proposed CTP Fundamental Rules, respondents provided feedback on:

- the scope of application of the CTP Fundamental Rules;
- the interpretation of CTP Fundamental Rules 3 and 6;
- suggested additional CTP Fundamental Rules; and
- enforcement of the CTP Fundamental Rules.

Scope of application of the CTP Fundamental Rules

2.61 Twenty-three respondents supported the regulators' proposal to apply the CTP Fundamental Rules in relation to all the services that CTPs provide to firms. Of these, three respondents highlighted potential difficulties if CTPs had to adopt different risk management approaches for their systemic and non-systemic third party services, respectively. They further outlined the potential for the effectiveness of the CTP Fundamental Rules to be limited if applied only in relation to the systemic third party services that CTPs provide to firms.

2.62 Conversely, ten respondents disagreed with the regulators' proposed scope of application for the CTP Fundamental Rules and suggested applying them only in relation to CTPs' provision of systemic third party services to firms, as these are the services whose failure or disruption could undermine the stability of, or confidence in the financial system. These respondents argued that their suggested scope of application for the CTP Fundamental Rules would be a more proportionate approach, and more in line with the Overall Objective.

2.63 The regulators acknowledge the need for the CTP Fundamental Rules to reflect the Overall Objective and be proportionate. The regulators acknowledge the potential burden on CTPs where they may be providing hundreds of services to the financial sector. With this in mind, the regulators have taken the decision to apply CTP Fundamental Rules 1 to 5 only in relation to CTPs' provision of systemic third party services to firms. However, this will be kept under review as the oversight regime develops.

2.64 To enable effective oversight of CTPs by the regulators, CTP Fundamental Rule 6 ('A CTP must deal with each regulator in an open and cooperative way and must disclose to each regulator appropriately anything relating to the CTP of which it would reasonably expect

notice') will apply in relation to all the services that a CTP provides to firms. Applying CTP Fundamental Rule 6 only in relation to a CTP's provision of systemic third party services to firms could unduly restrict the regulators' ability to receive information relevant to their oversight functions from CTPs. Without this information, the regulators may not be able to oversee CTPs effectively, or take the necessary steps to mitigate risks.

CTP Fundamental Rule 3

2.65 Six respondents requested clarification on the concept of 'prudent' in Fundamental Rule 3 ('A CTP should act in a prudent manner'). Of these, one queried whether the word 'prudent' should be interpreted as financially prudent.

2.66 One respondent recommended the removal of CTP Fundamental Rule 3 altogether. The respondent noted that CTP Fundamental Rule 3 appeared to have been lifted directly from the PRA's Fundamental Rules for dual-regulated firms, which are subject to additional, detailed prudential requirements (eg on capital, liquidity etc) that will not apply to CTPs. The respondent argued that it was unclear what 'acting in a prudent manner' meant for a CTP if these detailed prudential requirements did not apply to CTPs.

2.67 The arguments for the removal of CTP Fundamental Rule 3 appear to be based on an incorrect interpretation of the rule, which is not confined or explicitly tied to the detailed prudential regulatory requirements applicable to firms. However, this feedback indicated a need for the regulators to clarify how the phrase 'acting in a prudent manner' should be interpreted in the context of the CTP oversight regime. Consequently, SS6/24:

- clarifies that CTPs should interpret the phrase 'acting in a prudent manner', and CTP Fundamental Rule 3 consistently with the Overall Objective; and
- includes non-exhaustive examples of what a CTP acting in a prudent manner might entail.

CTP Fundamental Rule 6

2.68 Five respondents requested clarification on the requirement in CTP Fundamental Rule 6 to 'disclose to a Regulator appropriately anything relating to the critical third party of which it would reasonably expect notice' (disclosure requirement). Of these:

- one respondent argued that it would be difficult for CTPs to determine which matters the regulators expected notice of, and suggested deleting the disclosure requirement;
- one respondent suggested that that the disclosure requirement should relate to matters that materially impact the ability of a CTP to provide services in a secure and resilient manner;
- one respondent questioned whether the disclosure requirement could clash with contractual clauses prohibiting or restricting a CTP's ability to disclose information relating

to its customer firms;
- one respondent requested clarification on whether the disclosure requirement applied in relation to a CTP's provision of non-systemic third party services; and
- one respondent requested examples of the type of information that CTPs would be required to disclose.

2.69 In light of this feedback, and to aid CTPs' understanding of the type of information envisaged by the disclosure requirement in CTP Fundamental Rule 6, SS6/24 includes a list of matters of which the regulators would reasonably expect notice. This list is non-exhaustive, and the regulators have clarified in the SS6/24 that CTPs should interpret the disclosure requirement in CTP Fundamental Rule 6 in light of the Overall Objective.

Other clarifications

2.70 Five respondents asked for clarity on the interpretation of other terms in the CTP Fundamental Rules, such as 'responsibly' and 'integrity'. The regulators have explained in SS6/24 that terms such as 'responsibly' and 'acting with integrity' should be given their ordinary meaning and interpreted in line with the Overall Objective.

Proposed additional Fundamental Rules

Openness and cooperativeness with customer firms

2.71 Eight respondents requested the inclusion of an additional CTP Fundamental Rule (or an extension of CTP Fundamental Rule 6) requiring a CTP to be open and cooperative with the firms it provides services to. Of these:

- five respondents asked for this additional suggested rule to also require CTPs to support firms in fulfilling their regulatory obligations;
- two respondents asked for the proposed new rule to require CTPs to disclose to its customer firms anything of which they would reasonably expect notice; and
- one respondent suggested that the new rule included a requirement for a CTP to manage conflicts of interest between it and its customers.

2.72 The regulators consider that the proposed additional CTP Fundamental Rule is unnecessary as their rules already include:

- a general requirement for a CTP to have in place effective and secure processes and procedures to ensure sufficient and timely information is given to the firms to which it provides any systemic third party services to enable them to manage adequately risks related to their use of these services; and

- requirements for CTPs to share specific information with these firms and report CTP operational incidents to them.

2.73 However, the regulators have amended SS6/24 to note that CTPs should comply with the requirements referred to above in an open and cooperative way, and in line with the spirit as well as the letter of the relevant rules. CTPs should adopt a ‘transparency by default’ approach with regards to this requirement. Examples of relevant information include, but are not limited to, summaries (prepared by the CTP) of key, relevant findings from skilled persons reports, and any remediation that the CTP proposes to undertake in response. When sharing relevant information with firms, the regulators recognise that there may be confidentiality and sensitivity issues to be taken into account.

Adequate financial resources and preparedness for resolution

2.74 Four respondents suggested an additional CTP Fundamental Rule requiring CTPs to maintain adequate financial resources. Of these:

- one respondent asked that the suggested rule include a requirement on CTPs to comply with financial regulations in all the jurisdictions in which they operate; and
- one respondent urged the regulators to ensure that the suggested, new CTP Fundamental Rule require CTPs to remain solvent and report material financial reporting weaknesses to the regulators.

2.75 Relatedly, two respondents suggested an additional CTP Fundamental Rule requiring CTPs to be prepared for resolution.

2.76 The regulators also view these suggested additional CTP Fundamental Rules as unnecessary, as these areas are adequately covered by the Operational Risk and Resilience Requirements examined in the next section. In particular, the regulators expect:

- under Requirement 2 that a CTP considers its financial resilience insofar as it can impact its provision of systemic third party services to firms;
- under Requirement 8 that a CTP takes steps to mitigate the potential impact of insolvency on its provision of systemic third party services to firms. Moreover, in the absence of a statutory resolution regime for CTPs, which does not currently exist, there’s a limit to the extent that the regulators could require a CTP to prepare for resolution.

Business Continuity Planning

2.77 One respondent requested an additional CTP Fundamental Rule requiring a CTP to ensure that services provided to firms are subject to regular business continuity planning and testing.

2.78 The regulators consider that the proposed CTP Fundamental Rule is also unnecessary. The Operational Risk and Resilience Requirements, in particular Requirement 7, already cover a CTP's incident management extensively. SS 6/24[11] further clarifies that a CTP should include business continuity as part of its suite of incident response and recovery measures. Furthermore, in keeping with the regulators' requirements on scenario testing and incident management playbook exercises a CTP is expected to assess the effectiveness of its incident management capabilities regularly.

Enforcement

2.79 Two respondents sought clarity on how CTPs would demonstrate compliance with the CTP Fundamental Rules. One respondent suggested that the regulators should provide examples of good practice. Two respondents, while expressing strong support for the CTP Fundamental Rules, advocated for sanctions to ensure effectiveness.

2.80 The regulators have provided greater clarity on their expectations of how CTPs should interpret and comply with aspects of the CTP Fundamental Rules, such as acting in a prudent manner (see paragraphs 2.65 – 2.67 above). The regulators' approach to enforcement under the CTP regime is the Bank's CTP enforcement SoP and the equivalent FCA Handbook enforcement SoP in Appendices 9 and 10 respectively of this PS.

CTP Operational Risk and Resilience Requirements

2.81 In Chapter 5 of CP26/23, the regulators proposed eight Operational Risk and Resilience Requirements that CTPs would be required to comply with in respect of their systemic third party services. The aim of the proposed Operational Risk and Resilience Requirements is to provide clear, consistent, outcomes-focused obligations that all CTPs would be required to meet in respect of these services.

2.82 Several respondents provided detailed feedback on the CTP Operational Risk and Resilience Requirements. Of those, the majority supported the proposed Requirements, with some expressly welcoming their alignment to: (i) the requirements for firms relating to operational resilience, and outsourcing/third party risk management; (ii) international standards; and (iii) industry best practice. One respondent noted that the positive impact of the Operational Risk and Resilience Requirements would lie in their collective contribution to fostering operational resilience among CTPs. Two respondents objected to the proposed Requirements, one of which asked that they be replaced with a requirement for CTPs to provide a statement of consistency with ISO standards **27001** and **27002**

2.83 Most respondents' detailed feedback focused on the following Operational Risk and Resilience Requirements:

- Requirement 1: Governance;
- Requirement 3: Dependency and supply chain risk management;

- Requirement 4: Technology and cyber resilience;
- Requirement 6: Mapping;
- Requirement 7: Incident Management; and
- Requirement 8: Termination of services

2.84 Having considered the responses, the regulators have decided to retain all the CTP Operational Risk and Resilience Requirements. These Requirements articulate the standards of resilience that CTPs will be required to maintain in respect of their systemic third party services and are therefore an essential part of the CTP oversight regime.

2.85 However, in response to feedback, the regulators have revised various CTP Requirements, or aspects thereof to make them clearer, more effective, and/or more proportionate.

2.86 Most respondents agreed with the proposal to apply the CTP Operational Risk and Resilience Requirements only in relation to CTPs' provision of systemic third party services to firms. The regulators have therefore made no changes to the scope of these Requirements.

Requirement 1: Governance

2.87 Three respondents noted that it may not be practical for CTPs to appoint just one individual as the point of contact for the regulators in respect of the exercise of their functions under the oversight regime ('point of contact'). They suggested that the regulators should either require CTPs to appoint at least one individual or give CTPs flexibility to appoint a team.

2.88 The regulators recognise that it might be necessary or desirable for CTPs to appoint more than one individual as point of contact and have amended their final rules and SS6/24 to give them flexibility to do so.

2.89 Four respondents noted that the regulators should provide additional guidance on their expectations of the experience, knowledge, seniority, and skills of the point of contact. One respondent argued that, as the CTP regime is new, the point of contact's experience and knowledge should cover the CTP's operations, but not financial regulation.

2.90 The regulators emphasise the need for the point of contact to have appropriate authority, knowledge, experience, and skills to carry out his/her/their role and have reflected this in their rules and SS6/24. The central point of contact's knowledge of financial regulation should be sufficient to enable a CTP to comply with its duties under the regime. However, the regulators recognise that this knowledge will develop gradually, and have added an expectation in

SS6/24 on CTPs to implement appropriate training of relevant financial regulation among the individual(s) acting as the central point of contact and, (to the extent appropriate) other areas of the CTP essential to the delivery of systemic third party services to firms.

2.91 Two respondents suggested that CTPs should be subject to the SM&CR or an equivalent individual accountability regime. This would allow the regulators to hold individuals at the CTP accountable for failures; ensure that a CTP's governing body and senior management paid appropriate attention and resources to the CTP regime; and promote parallel standards to those applicable to firms.

2.92 The application of the SM&CR is governed by **Part V of FSMA** which does **not** extend to CTPs. Therefore, the regulators cannot apply the SM&CR to individuals in CTPs. However, certain features of Requirement 1 have been partly inspired by elements of the SM&CR, such as the requirements on a CTP to:

- establish clear roles and responsibilities at all levels of their staff essential to the delivery of a systemic third party service, with clear and well-understood channels for communicating and escalating issues and risks; and
- ensure appropriate review and approval of any information provided to the regulators.

Requirement 3: Dependency and supply chain risk management

2.93 Requirement 3 generated extensive feedback. Four respondents singled it out as particularly useful. One respondent noted that ensuring appropriate transparency from CTPs about their sub-contractors and wider supply chain had long been a pain point for firms and argued that supply chain robustness would be particularly beneficial for the financial sector.

2.94 Four respondents raised concerns about a lack of proportionality in certain aspects of Requirement 3 and suggested: limiting its scope to Key Nth Party Providers (as defined in the rules and section 2 of SS6/24); and making some of the obligations for CTPs under this Requirement less onerous.

2.95 In response to this feedback, the regulators' final rules and SS6/24 have made Requirement 3 more proportionate while ensuring it remains effective to manage supply chain risks, which are a major, recurrent source of incidents at third party service providers. The regulators have done so by maintaining the general requirement for CTPs to identify and manage supply chain risks to systemic services whilst limiting some of the specific requirements to Key Nth party providers and Persons Connected to a CTP. The regulators have also broadened Key Nth party providers by removing 'service' as consulted on in CP26/23. The change will ensure a CTP captures all providers that are essential to the delivery of a systemic third party service to one or more firm.

2.96 Two respondents noted that any requests or requirements on a CTP to disclose information about its supply chain should: consider confidentiality and security issues, such as the protection of confidential or sensitive information about non-CTPs, personal data, trade secrets etc; and exclude non-relevant information.

2.97 The regulators have acknowledged in SS6/24 that, when sharing information regarding their supply chain, a CTP may need to consider confidentiality and security issues. They have also noted that, when deciding what information to share about its supply chain, a CTP should consider: the relevance of this information to the Overall Objective and its duties under the regime (including but not limited to CTP Fundamental Rule 6 and Requirement 3); and ways to protect confidential or sensitive information while complying with these duties. Consistent with the Overall Objective and CTP FR 6, a CTP should not simply use confidentiality or security as blanket excuses to refuse to share information with regulators on its supply chains.

Requirement 4: Technology and cyber resilience

2.98 One respondent suggested that Requirement 4 (Technology and cyber resilience) should be deleted on the basis that: (i) other requirements, such as Requirement 2 (Risk Management) and Requirement 7 (Incident Management) already captured its intended outcomes; and (ii) technology and cyber resilience should not be considered in a silo. Alternatively, if Requirement 4 was to be kept, the same respondent asked the regulators to clarify that a CTP could comply with it by complying with the remaining Operational Risk and Resilience Requirements, and/or through recognised certifications, such as ISO 27001: (Information Security) and 22301 (Business Continuity).

2.99 The regulators consider Requirement 4 a key Operational Risk and Resilience Requirement and have kept it in their rules. Cyber and technology risks have unique characteristics that warrant individual consideration. In addition, respondents to the Bank's biannual **Systemic Risk Survey** continue to identify the risk of a cyber-attack as one of the top risks that would have the greatest impact on the UK financial system if it were to materialise. It would be contrary to the Overall Objective not to consider cyber and technology risks explicitly in the CTP Operational Risk and Resilience Requirements.

2.100 The draft rules and SS6/24 in CP26/23 already clarified that 'all Operational Risk and Resilience Requirements are relevant to a CTP's cyber and technology risk management' and linked Requirement 4 to other Operational Risk and Resilience Requirements eg 2 and 7. The regulators have reiterated in the final SS6/24 that 'CTPs should manage all relevant risks as part of its risk management processes under Requirement 2 and avoid undue silos'.

2.101 The regulators have also explained in SS6/24 that a CTP's compliance with recognised standards can provide partial supporting evidence of its compliance with Requirement 4. For instance, by confirming that certain cyber-security controls are in place. However, recognised standards will not always provide all the assurance that the regulators need. For instance, on the effectiveness of those cyber-security controls. CTPs may therefore need to provide additional assurance that they are complying with Requirement 4.

2.102 Two respondents made a series of drafting suggestions to make Requirement 4 more proportionate, which the regulators have accepted. For instance, by requiring CTPs to take 'reasonable steps' to ensure the resilience of any technology that delivers, maintains or supports a systemic third party service, instead of stating that they 'must' ensure resilience (as CP26/23 originally proposed).

Requirement 6: Mapping

2.103 Various respondents asked the regulators to clarify explicitly that the CTP Operational Risk and Resilience Requirements apply to any resources that CTPs identify as essential to the delivery of systemic third party services in their mapping. Doing so would ensure that CTPs considered the resilience of these resources.

2.104 The regulators' draft rules in CP26/23 were always intended to apply to anything that may impact the resilience of a CTP's systemic third party services to firms. This implicitly includes resources essential to the delivery of those services. However, the regulators have made this point clearer in SS6/24.

2.105 Two respondents noted that a CTP's mapping should include 'internal essential services', which they described as those assets and technologies that support systemic third party services. Respondents argued that the failure of internal essential services could have a significant impact on a CTP's delivery of systemic third party services and highlighted previous incidents at third parties that had originated in failures to internal essential services such as domain name systems (DNS), security certificates or identity and access management. Respondents argued that ensuring that CTPs consider the resilience of internal essential services should be a core objective of the Operational Risk and Resilience Requirements.

2.106 The regulators have made it explicit in their rules and SS6/24 that services such as DNS should be mapped under Requirement 6 and are in scope of the requirements in the regulators' rules, such as those relating to testing. However, the regulators have not adopted the term 'internal essential services' in their rules or SS6/24 to avoid creating unnecessary additional terminology.

2.107 One respondent suggested that:

- mapping of resources and dependencies should be proportionate to the risk to the CTP's inability to deliver the systemic third party service;
- the regulators should acknowledge that mapping is only one possible input that a CTP may use to identify dependencies and potential areas for improvement; and
- Requirement 6 should be revised to:
  - permit CTPs to develop their own approach to mapping; and
  - clarify that alternative approaches may be used by a CTP if they achieve the same outcome as the mapping requirements.

2.108 In response to this feedback, the regulators have clarified in the SS6/24 that:

- each CTP is responsible for: (i) developing its own mapping methodology: and (ii) identifying the resources essential for delivering, supporting and maintaining its systemic third party services;
- a CTP's mapping should be proportionate to the nature, scale and complexity of its business; and
- a CTP may use additional tools to complement its mapping and meet the outcomes in Requirement 6, eg;
  - historical data to identify the parts of their supply chain most susceptible to disruption; or
  - inventories of information and other associated assets to populate the relevant parts of their maps.

2.109 However, the regulators have also clarified in SS6/24 that, irrespective of the approach chosen, a CTP's mapping should meet the outcomes in the regulators' rules and SS6/24.

2.110 One respondent noted that mapping will be important, but difficult, in long supply chains and asked the regulators to set more specific expectations about the broad types of data CTPs will be required to provide, including supply chain-specific mappings. SS6/24 sets out the regulators' expectations and other guidance to assist CTPs in their mapping. The regulators view this guidance as appropriate and proportionate and consider that additional guidance could be counterproductive by forcing a one-size-fits-all approach to mapping for all CTPs.

2.111 One respondent sought clarification as to whether a CTP's mapped assets and resources would need to be reflected in the mapping of the firms that the CTP provides services to. Requirement 6 is addressed to CTPs. However, as stated in SS1/21 – **Operational resilience: Impact tolerances for important business services**, firms may ask third parties to provide mapping, but this is not required in all cases, particularly if other assurance mechanisms are effective and more proportionate.

Requirement 7: Incident Management

2.112 Requirement 7 attracted some of the most detailed feedback of the whole CP. Respondents focused primarily on the proposed requirements for a CTP to set a maximum tolerable level of disruption for its systemic third party services and maintain and operate a Financial Sector Incident Management Playbook.

Maximum tolerable of disruption

2.113 There was extensive feedback on the proposed requirement for a CTP to set a maximum tolerable level of disruption for each of its systemic third party services. In particular, on the expectation in the draft supervisory statement that this maximum tolerable level of disruption should take into account and (to the extent possible) be compatible with the impact tolerances that firms have set for any IBSs that are supported by the systemic third party service(s) that the CTP provides.

2.114 Several respondents noted that it might be impossible for a CTP to link its maximum tolerable level of disruption for systemic third party services to the impact tolerances of the IBSs of customer firms that these services support because: impact tolerances for the same or similar IBSs may vary among firms; and a CTP may not know which IBSs their systemic third party services support and/or the impact tolerances that its customers have assigned to their IBSs. Some respondents also expressed reservations about the possibility of firms having to disclose detailed information about their IBSs to the CTPs they receive systemic third party services from, due to both the reporting burden on these firms and confidentiality concerns.

2.115 As an alternative, several respondents suggested that CTPs should:

- set a maximum tolerable level of disruption for their systemic third party services based on their choice of metrics (eg recovery time objectives (RTOs), Recovery Point Objectives (RPOs), service level agreements (SLA), service level objectives (SLOs) etc);
- share their maximum tolerable level(s) of disruption with the firms they provide systemic third party services to. This would enable these firms to assess a CTP’s maximum tolerable level of disruption against the impact tolerances of any IBSs that rely on the CTP’s systemic third party services, thus fostering alignment between the respective regulatory obligations of firms and CTPs; and
- one respondent suggested a further alternative whereby, following designation by HMT, the regulators could give a CTP anonymised information on the lowest impact tolerance that each of its systemic third party services supported based on information collected from firms.

2.116 One respondent suggested that the requirement for CTPs to set a maximum tolerable level of disruption should be removed as (in its experience) testing a service past the point of expected failure did not provide significant learning opportunities. Instead, the respondent suggested encouraging a CTP to focus on its ability to meet the service level commitments in its third party arrangements with customers, including firms.

2.117 The requirement for a CTP to set an appropriate maximum tolerable level of disruption is necessary to identify the timeframe and, if appropriate, other metrics within which the impacts of not resuming a systemic third party service would become unacceptable to that CTP in light of the Overall Objective. The notion of a maximum tolerable period of disruption already features in recognised standards such as ISO 22301 (Business Continuity). However, the regulators agree that a CTP's appropriate maximum tolerable level of disruption should promote continuous improvement to the resilience of a CTP's systemic third party services. The regulators have inserted the word 'appropriate' before 'maximum tolerable of disruption' in their rules and SS6/24 to illustrate the importance of this continuous improvement.

2.118 The regulators have also amended their rules and SS6/24 to note that:

- a CTP should use appropriate metrics and targets when setting an appropriate maximum tolerable level of disruption for its systemic third party services. It is up to the CTP to identify these metrics and targets. However, the CTP should:
  - take into account the Overall Objective;
  - include at least one time-based metric;
  - consider additional, non-time-based metrics, if appropriate; and
  - cover the end-to-end delivery of the systemic third party service in both business-as-usual and periods of heightened or peak activity.
- to inform the setting of its appropriate maximum tolerable level of disruption, a CTP should encourage the firms it provides systemic third party services to identify which of their systemic third party services are key to the resilience of their IBSs and, where possible indicate the recovery times they would expect for those systemic third party services;
- a CTP must share its appropriate maximum tolerable level of disruption for each systemic third party service with the firms it provides these services to; and
- a CTP may agree stricter service levels in its contractual arrangements with firms and test their systemic third party services against these stricter service levels in addition to testing them against their appropriate maximum tolerable level of disruption.

Incident management playbook

2.119 Most respondents supported the purpose behind the proposed financial sector incident management playbook, which is for a CTP to consider, plan, document, test, and review how it will communicate with and support their firm customers (individually and collectively), and the regulators during an incident. One respondent suggested that the playbook should include direct outreach mechanisms for firms known to be critically impacted by an incident.

2.120 One respondent emphasised the importance of the regulators being pragmatic and allowing each CTP flexibility in how it complies with the requirement for a financial sector incident management playbook. Three other respondents noted that requiring a CTP to develop a financial sector incident management playbook distinct from its existing documented incident management procedures would be disproportionate and increase operational risk. These respondents asked the regulators to allow a CTP to rely on its existing documented incident management procedures (with amendments or enhancements as required) if they met the intended outcomes of Requirement 7. Consequently, the regulators have replaced the requirement for a CTP to produce a 'financial sector incident management playbook', with a requirement to produce an 'incident management playbook'. The term 'incident management playbook' is an umbrella term for any document(s) which set out the CTP's incident management procedures. CTPs may use other names internally.

2.121 The rules specify the outcomes that a CTP's incident management playbook must achieve. The regulators have also provided additional further detail in SS6/24 on how CTPs' incident management playbook are expected to meet these outcomes. For instance, these playbooks should:

- ensure that CTPs have an appropriate, documented, effective, and regularly assessed process to communicate and cooperate with the regulators and the firms they provide systemic third party services to during a CTP Operational Incident; and
- facilitate and inform the development and testing of the business continuity plans of firms that receive systemic third party services from that CTP by improving their understanding of that CTP's incident management procedures.

2.122 Several respondents suggested that a CTP should be required to share its incident management playbook with the firms it provides systemic third party services to. The regulators consider that this could create undue risks, as these playbooks may contain information that is confidential and not relevant to firms. However, firms will get an appropriate level of visibility into CTP's incident management playbooks through other means, notably their participation in incident management playbook exercises.

2.123 One respondent noted that the proposed expectation for a CTP to 'coordinate incident communications with firms' would not be feasible, since CTPs may not have all information that may be relevant to firms' own incident response arrangements. In response, the

regulators have replaced this with an expectation in SS6/24 for a CTP to 'support affected firms, and the regulators to mitigate risks to the stability of, and confidence in, the financial system (eg by supporting their crisis communications if appropriate)'.

2.124 Two respondents noted that CTPs' incident management should not substitute bilateral support from a CTP to individual firms affected by a CTP operational incident. The regulators have clarified in SS6/24 that the requirements on a CTP to support the firms it provides systemic third party services to collectively apply in addition and without prejudice to any individual support that a CTP may provide to individual firms affected by a CTP operational incident in line with its contractual obligations.

Coordination with collective incident response frameworks

2.125 One respondent commented on the regulators' requirement for a CTP to 'coordinate and engage with arrangements put in place by firms, authorities, or other persons for coordinating responses to incidents adversely affecting the UK's financial sector or parts of it'. These arrangements (renamed Collective Incident Response Frameworks in the final policy to promote clarity) include the:

- **Authorities' Response Framework** (ARF), which is a formal way for the regulators and HMT to co-ordinate with each other when there is an incident or threat that could cause a major disruption to financial services; and
- Sector Response Framework (SRF), which is owned and maintained by the Cross-Market Operational Resilience Group (CMORG).

2.126 The respondent suggested that CTPs should be able to comply with the requirement to 'coordinate and engage with arrangements, or parts of it' by complying with the incident reporting requirements examined below. The respondent further noted that some CTPs, due to their operating model, will not know all the information that might be relevant to firms' incident response arrangements. Without this knowledge, those CTPs might be forced to speculate as to how best to coordinate and engage with collective incident management frameworks.

2.127 The regulators have not taken this suggestion forward. During a CTP Operational Incident, there is likely to be information and support that a CTP can provide collectively to affected firms that can significantly help the financial sector's response and recovery (in addition and without prejudice to tailored support that the same CTP may offer its individual customers). Given the likelihood of CTP Operational Incidents affecting the financial sector or part of it, it is essential that every CTP engages with Collective Incident Response Frameworks. A lack of awareness about how a CTP Operational Incident may affect individual customer firms does not prevent a CTP from engaging with these frameworks nor diminish the benefits of doing so.

2.128 Engagement with Collective Incident Response Frameworks during a CTP operational incident is also likely to benefit the CTP in practice, as these frameworks can centralise information-sharing and support to affected firms thus reducing the number of requests to a CTP for substantially the same information by individual firms.

2.129 To assist CTPs' future cooperation with Collective Incident Response Frameworks, 'Collective Incident Response Framework' is now a defined term in the rules. SS6/24 also clarifies that for the purposes of Requirement 7 'cooperation' should involve a CTP using pre-agreed, documented, and appropriately validated ways to communicate with and support one or more Collective Incident Response Frameworks during a CTP operational incident, so that the CTP can provide appropriate updates and support to affected firms and the regulators. The regulators have also noted that cooperation should take place:

- periodically prior to and in preparation for a future CTP Operational Incident, including, but not limited to, through incident management playbook exercises;
- during a CTP operational incident; and
- following the resolution of a CTP operational incident, to agree and embed lessons learnt from the incident and remediation actions.

2.130 One respondent recommended establishing a subject expert group to mitigate the challenges of developing CTP's incident management playbooks and assessing their effectiveness, and other technical aspects of the regime such as scenario testing. The regulators cannot mandate the creation of such a group, specify what form it should take or what activities it should carry out. However, the regulators would view the establishment of such a group or groups, including as part of existing Collective Incident Response Frameworks, as a very positive step.

Requirement 8: Termination

2.131 Several respondents recommended aligning Requirement 8 with the requirements and expectations for firms relating to outsourcing and third party risk management. In particular, on stressed exit planning. Respondents noted that:

- regulators should ensure that CTPs work closely with firms to develop exit plans. Two respondents suggested that CTPs should be required to develop stressed exit plans mirroring those of firms; and
- CTPs should be required to take reasonable steps to not disrupt or discourage the termination of a systemic third party service by its firm customers, or the transfer of this service to another third party. For instance, through deliberate commercial or technology impediments.

2.132 One respondent noted that Requirement 8 could be misinterpreted as requiring a CTP to transfer or allow the transfer of its intellectual property to another service provider, or to the firms' exiting the arrangement, and noted that this could give rise to adverse unintended consequences. The respondent suggested changing the term 'any relevant assets' to 'any relevant firm-owned assets' in the rules and SS6/24 to avoid misunderstanding. The regulators have included an appropriate clarification in the rules.

2.133 Another respondent asked the regulators to delete the requirement for CTPs to return assets, such as data, belonging to firms 'in an easily accessible format'. The respondent noted that this requirement was unclear as, in some cases, it might not be within the CTP's ability to return certain assets to its firms' customers in an easily accessible format. For instance, if firms store their data on a CTP's infrastructure, have encrypted that data and retain sole control of the encryption keys, it might not be possible for the CTP to return that data to those firms in decrypted form following termination.

2.134 In response to this feedback, the regulators have clarified in SS6/24 that 'firms remain responsible for complying with applicable requirements and expectations on operational resilience, and outsourcing, and third party risk management, including in relation to stressed exit strategies. Requirement 8 seeks to ensure that CTPs facilitate firms' compliance with these requirements but does not replace them'. For CTPs, this involves providing reasonable support to firms following the termination of a systemic third party service, and during any transitional period thereafter, and not putting in place undue barriers to disrupt or discourage the orderly termination or transfer of the systemic third party service. However, it does not require a CTP to transfer ownership or grant use of its intellectual property to another third party, or to relevant firms beyond what is necessary to ensure an orderly termination and transition.

2.135 The regulators have also clarified in SS6/24 that the phrase 'in an easily accessible format' is limited to actions within a CTP's reasonable control. For instance, if a firm has encrypted data stored by a CTP and has sole control of the encryption keys, Requirement 8 does not require the CTP to decrypt the data prior to returning it to the firm.

2.136 One respondent queried whether Requirement 8 could conflict with the duties and powers of court-appointed insolvency practitioners in the event of termination of a CTP's systemic third party services due to insolvency. The regulators have clarified in SS6/24 that, where termination is due to an insolvency, Requirement 8 continues to apply. However, a court-appointed insolvency practitioner may apply for a waiver or modification of this rule or any aspects thereof it would like to disapply under s138A and s138BA of FSMA. In any event, the actions that a CTP is required to take under Requirement 8 should be carried out before any actual insolvency as part of its insolvency planning.

2.137 One respondent suggested that: a CTP should provide adequate notice before discontinuing a service and, if a CTP replaces a systemic third party service with a new or upgraded service, the new service should be deemed automatically systemic. The regulators agree with this statement and would reasonably expect notice of such an important change to the provision of a systemic third party service under CTP Fundamental Rule 6. The CTP approach document notes that the regulators will review the systemic third party services a CTP provides, and notify HMT and CTPs where it identifies possible new systemic third party services.

Self-assessment, scenario tests, incident management playbook exercises and information sharing

2.138 In Chapter 6 of CP26/23, the regulators proposed to require CTPs to comply with a range of assurance, exercising, information-gathering and testing requirements.

Self-assessment

2.139 In Chapter 6 of CP26/23, the regulators proposed to require each CTP to:

- submit a written self-assessment to the regulators within three months of designation, and annually thereafter; and
- share a summary of the information contained in their self-assessments with its customer firms.

2.140 These proposals generated a lot of feedback, with evident divergences between third party respondents and firms. The former broadly supported the proposed requirement but were concerned about the security of the information they would be required to share and the three-month deadline for submitting their first self-assessment. The latter strongly supported the proposed requirement and wanted to maximise the amount of information and assurance they would receive from CTPs.

Deadline for submitting the first self-assessment

2.141 Five respondents raised concerns over the ability of a CTP to prepare and submit its first self-assessment within three-months of designation. Two respondents suggested a six-month deadline, and two others suggested a twelve-month deadline for submitting the first self-assessment (starting from the date specified by HMT in the designation order).

2.142 Respondents also noted that developing this first self-assessment would be a learning process and the resulting document might be of a lower standard than subsequent, annual self-assessments. For these reasons, respondents argued that sharing this first self-

assessment with the firms a CTP provides systemic third party services to, could give rise to unjustified concerns among these firms. In particular, if the regulators kept the proposed three-month deadline.

2.143 The regulators acknowledge that the proposed three-month deadline will be challenging for CTPs. However, the first self-assessment that CTPs will need to submit to the regulators will fulfil an important and unique role in the CTP oversight regime, which justifies keeping the three-month deadline.

2.144 In response to industry feedback, the regulators have differentiated the first self-assessment (renamed 'interim self-assessment') from subsequent annual self-assessments in their rules and SS6/24. For instance, SS6/24 clarifies that the purpose of interim self-assessments is for the regulators to get an early indication of the extent to which a CTP is able to meet the CTP duties at the time of designation by HMT and identify areas to prioritise in the early phase of oversight. Interim self-assessments are therefore an initial, diagnostic tool that will help make the regulators' oversight of CTPs more proportionate and targeted. As the CTP approach document notes, the regulators' interaction with a CTP in the year beginning with its designation and culminating in its first Annual Review, will generally be different to subsequent, regular oversight. The focus in this initial period will be on helping regulators better understand the CTP, with the objective of forming an initial view of the key risks it poses to their objectives. The interim self-assessment will be an integral tool in this early stage of engagement.

2.145 The regulators also acknowledge that a CTP's interim self-assessment might be less comprehensive and polished than its subsequent annual self-assessment, and that a CTP might be unable to demonstrate full compliance with all the requirements in the regulators' rules in its interim self-assessment. Therefore, the regulators have removed the requirement for a CTP to share its interim self-assessment with the firms it provides systemic third party services to. A CTP will still be required to share its subsequent, annual self-assessments with those firms.

Sharing the self-assessment with firms

2.146 Four respondents suggested that the regulators should require a CTP to share its full self-assessments with the firms it provides systemic third party services to (with confidential or sensitive information redacted where appropriate) instead of a summary of those self-assessments (as proposed in **CP26/23**). This would ensure that firms receive consistent information from CTPs. Respondents argued that a summary of the self-assessment could be too vague and might not give firms enough information on areas such as testing performed by the CTP. In contrast, one respondent noted that a summary of the self-assessment could

be sufficient, but the regulators should specify what information it should contain. Another respondent suggested that a CTP should agree the contents of its summary self-assessment with regulators before sharing it with firms.

2.147 Conversely two respondents did not support the proposal for a CTP to share even a summary of its annual self-assessment with the firms it provides systemic third party services to. One of these respondents argued that the security risk of a CTP sharing too much information with its customer firms would outweigh any benefits of doing so. The respondent further argued that this requirement could lead to a CTP providing only high-level information in the self-assessments submitted to the regulators.

2.148 Another respondent agreed with the intent behind the proposed self-assessment, but did not believe it would provide a strong enough incentive for continuous improvement by CTPs. Instead, the respondent recommended regular assurance reviews of CTPs to be undertaken by independent parties.

2.149 In response to this feedback, the regulators' final rules will require a CTP to share the full annual self-assessment submitted to regulators (with confidential or sensitive information redacted as appropriate) with the firms it provides systemic third party services to. The regulators consider this a balanced approach, which:

- mitigates the risk of CTPs providing insufficient information to the firms they provide systemic third party services to;
- reduces the number of documents that a CTP will need to produce, thus limiting the compliance burden; and
- gives a CTP the ability to redact confidential or sensitive information, thereby allowing it to mitigate security risks of over-sharing.

2.150 The regulators have chosen not to mandate routine, regular independent external assurance of CTPs. However, their ability to order skilled persons reviews of CTPs enables them to achieve an equivalent outcome on a case-by-case basis where justified (SS7/24).

Content of the self-assessment

2.151 Several respondents requested further guidance on the information and format of the self-assessment.

2.152 Regulators do not intend the self-assessment to be a 'tick box' exercise so it would not be appropriate to provide excessively granular criteria on how a CTP should complete them. However, in response to feedback, the regulators have:

- set out common expectations for interim and annual self-assessments, and updated Box 2 'Information for CTPs to include in their self-assessment' with additional guidance in

SS6/24; and

- clarified how the regulators will use self-assessments in CTP approach document.

Scenario testing

2.153 Most respondents supported the regulators' proposal for a CTP to carry out regular scenario testing of its ability to continue providing each systemic third party service within its appropriate maximum tolerable level of disruption in the event of a severe but plausible disruption to its operations.

2.154 One respondent recommended that scenario testing should test the ability of CTPs to meet service level commitments rather than their appropriate maximum tolerable level of disruption. The regulators have clarified in SS6/24 that a CTP may perform its scenario testing against stricter thresholds, in addition to its appropriate maximum tolerable level of disruption.

2.155 Several respondents provided comments and questions on how severe but plausible scenarios would be selected. In particular, they:

- asked whether these scenarios should be selected by the CTP, the regulators, the firms the CTP provides systemic third party services to, collective incident response frameworks or a combination of the above;
- suggested that scenarios should regularly consider:
  - continuity of service provision;
  - the failure or disruption of 'internal essential services';
  - the stressed exit of a key Nth Party Provider; and
  - climate related events, and disruption to a CTP's energy supply.

2.156 In response to these comments, the regulators have provided additional guidance on scenario-testing in SS6/24, which outlines their expectations on how CTPs should approach scenario selection; and the calibration of severity and plausibility of scenarios. The regulators have also clarified that scenario tests should be performed at least annually, but might be performed more frequently if warranted (or if the regulators request or direct it).

Incident management playbook exercise

General

2.157 Most respondents supported the proposed requirement for CTPs to test their incident management playbook with their firm customers through scenario-based exercises (referred to as 'incident management playbook exercises' in the final rules). However, multiple

respondents raised comments, concerns, questions and suggestions about how these exercises would and should work in practice. In particular, on:

- the distinction between the scenario-testing requirements in the previous section, and the requirement for CTPs to carry out incident management playbook exercises;
- participation by firms in these exercises. In particular:
  - whether such participation should be mandatory; and
  - what will constitute ‘an appropriate representative sample’ of firms;
- the format of exercises eg tabletop exercises etc; and
- how remediation by the CTP of areas for improvement identified through incident management playbook exercises would be followed up, and by whom.

2.158 One respondent argued that CTPs should not be required to assess the effectiveness of their incident management measures with a sample of their firm customers, but that a better outcome could be achieved with information-based cooperation between CTPs and firms. The respondent suggested that CTPs should conduct internal testing without participation of their firm customers.

2.159 The regulators are retaining the requirement for CTPs to carry out incident management playbook exercises with a sample of the firms they provide systemic third party services to. Incident management playbook exercises are vital for a CTP to manage the risks it poses to the stability of, or confidence in, the UK financial system, and demonstrate compliance with its duties under the CTP oversight regime. The main aim of these exercises is to assess the effectiveness of a CTP’s incident management playbook and promote its continuous improvement by deploying it in a simulated, scenario-based CTP operational incident with a sample of the firms that the CTP provides systemic third party services to. This will allow CTPs, and these firms to collaboratively identify and remediate areas for improvement in the way a CTP communicates with and supports its customers during a CTP operational incident.

2.160 The collaborative nature of incident management playbook exercises distinguishes them from other exercises and tests that a CTP may carry out to assess the effectiveness of its incident management procedures. For instance, recognised standards such as ISO/22301 already require organisations to implement and maintain an exercise programme to validate the effectiveness of their business continuity strategies and solutions. However, as highlighted by the respondent above, CTPs tend to perform these internal exercises with the only external input being that of external auditors in certain circumstances. By definition, internal exercises and tests do not allow a CTP to receive feedback on how to improve its incident management playbooks from external stakeholders, including the firms that would be affected by a CTP operational incident. Similarly, a CTP’s customers can sometimes perform

business continuity tests and exercises on their assets (applications, data) stored in a CTP's environment. While this is important to ensure that individual firms configure and use a CTP's services resiliently, this type of testing also does not involve active collaboration between a CTP and its customers.

2.161 However, the regulators recognise the need for greater clarity and detail on how incident management playbook exercises will work in practice, which they have included in SS6/24. The regulators have also clarified the main aim of incident management playbook exercises in their rules; distinguished exercises from scenario-testing; and made certain aspects of these exercises more proportionate for all parties involved.

Distinguishing incident management playbook exercises from scenario tests

2.162 One respondent argued that the scenario-testing requirements for CTPs examined in the previous section and the requirement for CTPs to carry out incident management playbook exercises should be treated separately, and differentiated more clearly in the rules and SS6/24.

2.163 Scenario tests and incident management playbook exercises have commonalities. They both involve the use of severe but plausible scenarios to simulate a CTP operational incident and assess the effectiveness of a CTP's incident management. The most notable difference is that incident management playbook exercises seek to assess and improve CTPs' ability to communicate with and support the firms they provide systemic services to during a CTP operational incident. Consequently, incident management playbook exercises require direct participation by a representative sample of these firms. The regulators have distinguished these two requirements by introducing 'incident management playbook exercise' as a defined term in the rules and stating the main aim of these exercises in the SS6/24.

Participation by firms and the regulators

2.164 Multiple respondents had questions and comments on how participation by firms in CTPs' incident management playbooks exercises would work in practice – in particular, whether participation would be mandatory, expected or voluntary.

2.165 Three respondents suggested that it should be made mandatory. One of those respondents noted that the regulatory objective of gaining a systemic view of resiliency and managing systemic risks would not be achieved if CTPs had to rely on voluntary participation by their firm customers.

2.166 Two other respondents asked whether the regulators would amend their operational resilience rules for firms in **SS2/21** and/ or the equivalent outsourcing and third party risk management SSs for **FMIs**, to compel firms to participate in the incident management

playbook exercises of any CTP they receive systemic third party services from. Several respondents asked how an appropriately representative sample of firms would be chosen, and who would determine its appropriateness (the regulators or the CTP).

2.167 In response to this feedback, the regulators have amended their rules and SS6/24 to:

- require CTPs to carry out the first of these exercises within the first twelve months of designation by HMT, and at least biennially thereafter (as opposed to annually, as proposed in CP26/23). This should help make these exercises less resource-intensive and facilitate participation by firms;
- clarify that CTPs should make participation in their incident management playbook exercises open to all the firms they provide systemic third party services to. However, they may select a sample of those firms, as part of outside support, to make the design and execution of the exercise more pragmatic and resource efficient;
- confirm that, for the time being, the regulators do not propose to make participation by firms in the incident management playbook exercises of the CTPs they receive systemic third party services from mandatory. However, as SS6/24 notes, participation is consistent with firms' regulatory obligations relating to operational resilience/ outsourcing and third party risk management, as well as in their own interest, particularly, if the services provided by the CTP performing the exercise are core to a firm's delivery of one or more important business services;
- provide guidance on the meaning of 'participation' by a firm in a CTP's incident management playbook exercise, which, at a minimum, entails:
  - attending the exercise;
  - considering the quality and timeliness of information and support provided by the CTP during the exercise, and other relevant aspects of its incident management playbook;
  - providing feedback to the CTP (directly or via the external party coordinating the exercise) on possible improvements to the above;
- note that firms can scale the level of participation at a CTP's incident management playbook exercise depending on factors such as its systemic significance, and the resources available to it; and
- explain that, although CTPs are accountable for running their incident management playbook exercises, they can use outside support from collective incident response frameworks and independent experts in the design and execution of these exercises. This support may include coordinating participation by firms to help the CTP achieve a representative sample, and identifying severe but plausible scenarios.

2.168 Some respondents suggested that the regulators should also participate in CTP's incident management playbook exercises. The regulators agree that there could be clear advantages to their participation in these exercises, but this needs to be balanced against the need for them to use their resources efficiently. The regulators have therefore noted in the CTP approach document that they may observe selected incident management playbook exercises. This will enable the regulators to:

- improve their own capabilities to coordinate with CTPs and firms during a CTP operational incident that affects the financial sector eg by invoking the ARF;
- identify ways to improve communication with CTPs and affected firms during CTP operational incidents; and
- identify potential gaps in the CTPs incident management processes.

2.169 To promote cross-border and cross-sectoral regulatory and supervisory interoperability, which was a major cross-cutting theme in responses (see 'Alignment to international standards and interoperability non-UK regimes' above), the regulators may also invite non-UK financial regulators and UK non-financial regulators, and public authorities that carry out similar functions or have overlapping mandates over CTPs to observe relevant CTPs' incident management playbook exercises. The regulators will give a CTP advance notice if they intend to observe an incident management playbooks exercise, either alone or with another authority.

Format of the exercises

2.170 Several respondents asked for additional guidance on the format of CTPs' incident management playbook exercises. In particular:

- three respondents suggested that the incident management playbook exercises should comprise tabletop exercises. The objective of these tabletop exercises should be to renew firms' understanding and validate existing assumptions about how a CTP would respond in the event of a CTP operational incident. This approach would allow for more frequent exercises, and participation by a larger number of firms; and
- several respondents suggested that the scenarios used in incident management playbook exercises should involve the failure or disruption of 'internal essential services' (see previous subsection), and the technology used to delivery systemic third party services.

2.171 In response to this feedback, the regulators have:

- provided a list of different objectives that incident management playbook exercises may fulfil, drawing on the **G-7 Fundamental Elements of Cyber Exercise Programmes** and

- clarified that a CTP is responsible for selecting the most appropriate type of incident management playbook exercise ahead of the next exercise and should discuss its choice with the firms that are due to participate and the regulators.

Recommendations and follow-up

2.172 Several respondents asked how CTPs would get feedback, including recommendations for improvement, from participating firms following an incident management playbook exercise, and how the regulators would monitor the implementation of these recommendations. One respondent cautioned that the outcomes of exercises may be interpreted differently across firms, making it difficult for CTPs to form a clear, corrective plan.

2.173 One respondent suggested that the report that CTPs will be required to prepare following each incident management playbook exercise should not be an additional requirement as this will already be included as part of their annual self-assessment.

2.174 The regulators have clarified in their rules and SS6/24 that at the end of an incident management playbook exercise:

- a CTP should collate feedback from participating firms and (where relevant) the regulators on how to improve its incident management playbook;
- a CTP must, as soon as is practicable, prepare and submit to the regulators a report of the incident management playbook exercise (including any actions taken in the light of the results of that exercise). A CTP's annual self-assessment should also include this report; and
- a CTP should update the regulators on the implementation of any changes as a result of its latest incident management playbook exercise no later than six months after the date of its most recent exercise.

Additional forms of testing

2.175 Among those respondents who commented on the possibility of additional mandatory forms of regular testing for CTPs, the great majority agreed that there should be no additional mandatory forms of regular testing beyond those already mentioned in the rules and SS. These respondents considered that such additional testing would be disproportionate and potentially unmanageable for CTPs to maintain.

2.176 One respondent suggested that the regulators have regular meetings with a CTP's internal and statutory auditors, as these parties may have further information that will inform the regulators' ongoing assessment of CTPs. The regulators have not made any additional changes to their final rules and SS6/24 in response to this point, as they already have a degree of recourse to a CTP's internal and statutory auditors, which they may exercise if appropriate.[12]

Incident reporting and other notifications

2.177 In Chapter 7 of CP26/23, the regulators proposed to require CTPs to notify them, and their firm and FMI customers who receive an affected service of certain incidents and other events.

2.178 There was extensive, detailed feedback to this part of the consultation. Most respondents welcomed the requirements for CTPs to report CTP operational incidents to affected firms and the regulators. The general view was that these reports would benefit firms, as they would enable them to respond and recover from incidents originating at a CTP more effectively.

2.179 As noted above, the regulators' final rules distinguish between incident reports, and other notifications. Both are examined in this section, which uses the new terminology.

Definition of relevant incident /CTP Operational Incident

Actual vs potential impact

2.180 Multiple respondents commented on the regulators' proposed definition of 'relevant incident'. Six respondents expressed concern that the phrase 'or has the potential to' in the definition made it too broad and could lead to an excessive and counterproductive number of incident reports, since many events have the potential to cause disruption but, ultimately do not. Three of these respondents suggested replacing the phrase 'has the potential to' with 'is highly likely to', while two suggested deleting it altogether, along with the phrase 'or the potential to result in a serious loss of such assets' from the definition of relevant incident.

2.181 The regulators consider these points to be appropriate and have amended the definition of 'relevant incident' (renamed 'CTP operational incident'). The definition of a 'CTP operational incident' in the final rules does not include the phrases 'or has the potential to result in any of those things.' It only applies to events with an actual impact on a CTP's provision of systemic third party services, or to its operations.

2.182 The regulators have also noted in SS6/24 and CTP approach document that:

- under CTP Fundamental Rule 6, they reasonably expect to be made aware of incidents that have not yet had an impact on a CTP's provision of systemic third party services or operations, but are highly likely to do so (as suggested by some respondents); and
- CTPs should report aggregate incidents and near-misses in their self-assessment. The regulators may also request these data on an ad-hoc basis if appropriate. The regulators are particularly interested in areas for improvement and other lessons that a CTP has learnt from these other incidents and near-misses, as well as any commonalities and trends in them.

Relationship with the definition of an ICT-related incident in DORA

2.183 One respondent suggested that the definition of relevant incident should align to the definition of ICT-related incident in Article 3(8) of DORA, notwithstanding that DORA does not apply in the UK. Although it is likely that some CTP operational incidents will lead to ICT-related incidents under DORA, full alignment between the two definitions is not appropriate because the requirement to report ICT-related incident in DORA is aimed at EU financial entities, not at critical ICT third party service providers, and CTPs will also be required to report non-ICT-related incidents meeting the definition of a CTP operational incident.

Interpretation of 'serious'

2.184 Four respondents raised concerns about the use of the words 'serious' and 'seriously' in the proposed definition of a relevant incident, which they noted were open to interpretation. They suggested that the regulators should either clarify how these words should be interpreted in the context of a CTP operational incident, or delete them. One respondent suggested that CTPs should assess the seriousness of a relevant incident by reference to the maximum tolerable level of disruption that they will be required to set for their systemic third party services.

2.185 Having considered this feedback, the regulators deem it appropriate to retain the notion of seriousness in the definition of a CTP operational incident to mitigate the risk of an unduly large volume of incident reports. However, in SS6/24, the regulators have clarified how they expect a CTP to assess seriousness, including but not limited to by reference to the appropriate maximum tolerable level of disruption that a CTP must set for each of its systemic third party services.

Impact on firm assets

2.186 Two respondents noted that some CTPs may not know whether an incident has impacted 'the availability, authenticity, integrity or confidentiality of assets relating or belonging to firms' which a CTP has access to because of the services it provides to these firms. These respondents argued that certain CTPs may not know how firms configure or use their services and explained that the extent to which an incident at a CTP can impact assets belonging to firms may vary depending on actions taken by those firms. For instance, whether they have encrypted the data they store on the CTP's infrastructure. Respondents also asked to delete the words 'relating to', which they found unclear.

2.187 The regulators have addressed this feedback in the revised definition of a CTP operational incident. In particular, the second part of the definition has been redrafted so that it encompasses an event or series of events that 'impacts a CTP's operations such that the availability, authenticity, integrity or confidentiality of assets belonging to firms which a CTP has access to as a result of it providing a systemic third party service to those firms is or may

be seriously and adversely impacted'. The use of 'or may be' highlights the fact that all CTPs will know if their operations (eg the security of their infrastructure) have been breached, but some may not know whether, as a result of this breach, the confidentiality, integrity, authenticity or availability of assets belonging to firms that use its systemic third party services has been adversely and seriously impacted.

Affected firm

2.188 Linked to the point above, 'affected firms' has been introduced as a defined term in the rules to provide clarity on the firms to whom a CTP must report CTP operational incidents. An affected firm means, in relation to a CTP operational incident:

- any firm to which a CTP supplies a systemic third party service impacted by that CTP operational incident; or
- any firm whose assets are or may be seriously and adversely impacted by that CTP operational incident.

Consistent use of CTP Operational Incident

2.189 As requested by several respondents, references to 'incident' and 'disruption' (in their ordinary meaning) throughout the rules and SS6/24 have been replaced with references to a 'CTP operational incident' to improve clarity and consistency. Disruption remains a defined term in its own right, and forms part of the definition of a CTP Operational Incident.

Reporting of CTP operational incidents to the regulators

2.190 One respondent objected to the proposed requirement for CTPs to report CTP operational incidents to the regulators, and noted that:

- Direct incident reporting by CTPs to the regulators could be counterproductive as certain CTPs may not know exactly how individual firms had been affected by a CTP operational incident. This impact may vary depending on how these firms configure and use the CTP's services, and any measures they may have taken to protect those assets.
- A requirement on CTPs to report incidents directly to the regulators would diverge from the approach taken by the EU in DORA and the US in the **Computer Security Incident Reporting Rule** neither of which require critical ICT third party service providers and bank service companies respectively to report incidents directly to the regulators, only to their financial services customers.

2.191 Several respondents also raised concerns about the amount of information that CTPs would be required to include in their incident reports, which went beyond what is currently required or expected from firms.

2.192 Having considered this feedback, the regulators have decided to keep the requirement for CTPs to report CTP operational incidents both to affected firms and the regulators. The regulators consider that it would be self-defeating to the Overall Objective not to have a mechanism for the regulators to be informed directly and promptly of CTP operational incidents.

2.193 The regulators will shortly be consulting on incident reporting requirements for firms, which have been designed to complement those that will apply to CTPs. In the event of a CTP operational incident that affects multiple firms, it is likely that both the CTP and affected firms will have unique information and insights about the incident. Receiving incident reports from both the CTP and affected firms in those cases will, far from being counterproductive, give the regulators a full picture of the incident and its impact on the financial sector. If the regulators did not require CTPs to report CTP operational incidents directly and promptly to them, their ability to respond to these incidents and coordinate with relevant stakeholders would be impaired.

2.194 Moreover, while the regulators are keen for the CTP oversight regime to be interoperable with similar non-UK regimes, this is only insofar and to the extent that interoperability does not undermine the Overall Objective of the regime, which would be the case if CTPs were not required to report CTP operational incidents directly to the regulators.

2.195 However, the regulators recognise that certain CTPs may have limited visibility on how CTP operational incidents they may experience will impact individual customers and have reflected this both in the definition of a CTP operational incident (see paragraph 2.185), throughout the incident reporting rules for CTPs, and in SS6/24. For instance, the regulators have removed from the incident reporting rules from the proposed requirements in CP26/23 for CTPs to include information in their incident reports that would have involved them having to speculate about the impact of a CTP operational incident on individual affected firms (if not known).

Phased approach to incident notifications

2.196 CP26/23 proposed a phased approach to CTP incident reporting comprising: (i) an initial incident report; (ii) one or more intermediate incident reports as needed; and (iii) a final incident report. This phased approach is consistent with the FSB's **Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report – Financial Stability Board** the FSB's ongoing work on a global **Format for incident reporting exchange** (FIRE), and DORA.

2.197 Most respondents supported the regulators' proposed phased approach to incident reporting, but raised several comments and questions.

Initial incident report

2.198 Respondents asked for clarity on the requirement to submit the initial incident report ‘without undue delay after a CTP is aware that the relevant incident has occurred’. Some respondents queried whether there should be a specific deadline for initial incident reports. Conversely, several respondents welcomed the proposal not to impose fixed time periods for incident reports. Several respondents also noted that:

- the timeliness of initial incident reports should take priority over their level of detail if there is a conflict between the two; and
- the information that CTPs must include in their initial and intermediate incident reports should not be so onerous as to unduly divert resources from withstanding, responding to and recovering from the incident.

2.199 In response to this feedback, the regulators:

- do not consider it appropriate to provide a fixed deadline for submitting initial incident reports given the variable complexity and nature of CTP operational incidents;
- have changed the requirement for CTPs to submit their initial incident reports ‘without undue delay’ to a requirement to submit them ‘as soon as practicable’ after the occurrence of a CTP operational incident; and
- have noted in SS6/24 that, if there is a conflict between the level of detail in a CTP’s initial report and the timeliness of the submission of that report to affected firms and the regulators, the CTP should prioritise timeliness and provide additional detail as necessary in later phases.

Intermediate incident report

2.200 There was mixed feedback on intermediate incidents reports. Some respondents argued that intermediate incident reports should not be required if a CTP operational incident was resolved quickly. Other respondents noted that, in some cases, an intermediate incident report may not be sufficient, for instance, in a CTP operational incident which took a long time to resolve or with an evolving impact. Several respondents encouraged the use of real-time or near real-time automated updates via dashboards and RSS feeds. One respondent suggested that a secure centralised repository could ease the burden on CTPs and potentially provide affected firms and the regulators with faster incident reports. In response to this feedback, the regulators have amended the draft rule instruments on which they consulted such that the regulators’ final rules:

- require CTPs to submit an intermediate incident report as soon as practicable after any significant change in the circumstances described in the initial incident report and (if applicable) any prior intermediate incident report. SS6/24 provides non-exhaustive examples of significant changes; and

- explicitly mention the incident being resolved as an example of a ‘significant change’ and clarify in SS6/24 that, if the only significant change since the initial incident report is the resolution of the incident, the intermediate incident report can simply involve making the regulators aware that the incident has been resolved.

2.201 SS6/24 notes that a CTP may use mechanisms, such as customer portals or RSS feeds to share information with customer firms during the lifecycle of an incident. However, reports to the regulators must include the information specified in the rules. This is necessary to ensure consistency and comparability in the information reported by CTPs during CTP operational incidents.

Final incident notifications:

2.202 The final rules and SS6/24 require a CTP to submit a final report within a reasonable time of the CTP operational incident being resolved. The regulators have decided not to mandate a specific timeframe for CTPs to submit their final report in the rules, but have indicated that they expect these final reports within 30 working days following the resolution of a CTP operational incident. Where a CTP requires longer than 30 working days, it should indicate to the regulators its intended date for submitting this report.

Contents of CTP incident reports

2.203 Most respondents supported the proposed contents of the various incident reports, but raised a number of queries and suggestions about specific items of information across three reporting phases.

Initial incident reports:

2.204 There was general support for most of the information that CP26/23 proposed a CTP include in its initial incident report.

2.205 Some respondents suggested removing ‘the cause or possible cause of the relevant incident, either known or suspected’ from the information to be included. The phrase ‘or suspected’ was particularly challenging for these respondents, who noted that it could force a CTP to speculate as to the possible cause of a CTP operational incident. This could in turn cause affected firms and the regulators to implement certain incident response and recovery that may not be appropriate if the suspected cause of the incident turned out to be incorrect.

2.206 Some respondents noted that the obligation for a CTP to appoint a designated point of contact for the regulators under Operational Risk and Resilience Requirement 1 rendered the proposed requirement for a CTP to name an individual responsible for communicating with the regulator during a CTP operational incident redundant.

2.207 In response to feedback, the regulators have streamlined the information to be included in the initial incident report to:

- reflect changes to the definition of a CTP operational incident. In particular, by removing the requirement for a CTP to provide information where assets relating or belonging to firms have as a result of the [CTP operational] incident been lost, compromised, corrupted, or become unavailable for a significant period. As noted above, certain CTPs may not know if this has been the case. Instead, a CTP is simply required to describe the CTP operational incident's impact on its operations;
- only include the cause of the incident if known at the time of submitting the initial incident report;
- remove the requirements for a CTP to provide the contact details of any individual(s) responsible for communicating with the regulators about the incident. A CTP must still provide details of the individual(s) responsible for communicating with affected firms; and
- encourage CTPs in SS6/24 to name individual affected firms as granularly as possible, while recognising that some CTPs may only be able to name the firm(s) they have a direct contractual relationship with.

Intermediate incident reports:

2.208 Most respondents agreed with the proposed contents of intermediate incident reports in the consultation.

2.209 The information that a CTP is required to include in its intermediate incident report has been made less granular. The regulators have also provided in SS6/24 examples of the type of information that may assist the regulators and affected firms in understanding the nature and extent of the CTP operational incident includes eg in the case of a CTP operational incident resulting from a cyber-attack.

Final incident notifications:

2.210 Respondents generally supported the proposed contents of final incident reports, which a number of respondents identified as a potentially valuable source of lessons learned.

2.211 One respondent commented removing suggested areas for improvement for firms from final incident reports on the basis it would not be appropriate for a CTP to provide every affected firm with recommendations for improvement aimed at other affected firms. The regulators have kept this requirement, but clarified in SS6/24 that the information that the CTP should include relates to areas for improvement for affected firms in general, rather than advice of guidance to individual affected firms, which they should continue to provide bilaterally and confidentially.

Standardised incident notification template

2.212 In CP26/23, the regulators asked for views on a standardised template for CTP incident reports. Several respondents supported the idea of a template, and noted that it could promote consistent reporting from CTPs, while also emphasising the need for flexibility. Some respondents suggested a voluntary template as a balanced approach.

2.213 Conversely, several respondents opposed the template as they considered that it would be unduly prescriptive and add to the extensive list of bespoke incident reporting requirements that many CTPs have to comply with already, in particular those that provide services in multiple jurisdictions and to other sectors in addition to financial services. One respondent noted not having a prescribed format provides CTPs flexibility and scope to provide information in the most appropriate and digestible format for their firm customers and the regulators based on the nature of the incident.

2.214 The regulators have decided to provide a voluntary incident reporting template in due course, which they consider will strike the right balance between promoting consistency and giving CTPs flexibility.

2.215 As noted in SS6/24. the information that CTPs are required to report to the regulators is likely to overlap with the information required by other authorities, at least partly. A CTP may therefore comply with its incident reporting obligations by leveraging incident reports (or relevant parts thereof) submitted to other authorities provided that these reports include the information required by the regulators' rules. A CTP should assess whether these reports meet the regulators' requirements and amend them as appropriate.

2.216 The regulators will monitor the effectiveness of their incident reporting rules for CTPs once the regime is implemented, and may review them to reflect lessons learnt in due course. This may include revisiting the case for a mandatory standardised incident notification template to promote comparable, consistent incident reporting. Making any potential future standardised incident notification template mandatory for CTP reporting would be subject to formal consultation.

Other matters

2.217 Some respondents also suggested that:

- CTPs should include general guidance for customers on incident mitigation. However, guidance to individual customers should remain bilateral and confidential;
- it would not be appropriate for CTPs to include updates on the potential impact of media coverage (including as a result of misinformation or disinformation). One respondent, however, suggested that they should include information on the actual impact.

2.218 The regulators agree with these suggestions and have reflected them in the rules and SS6/24. For instance, the proposed requirement for CTPs to include updates on media commentary relating to a CTP operational incident, has been replaced with an expectation on the CTP to outline any steps it has taken or proposes to take to address misinformation and disinformation relating to the CTP operational incident in the mainstream or social media.

Other notifications

2.219 In CP26/23, the regulators consulted on proposed requirements for CTPs to notify the regulators of other matters in addition to CTP operational incidents (see CP26/23 paragraph 7.20).

2.220 One respondent noted that the proposed notification requirements should only apply if the events listed above seriously and adversely impact or could seriously and adversely impact the CTP's ability to deliver any of its systemic third party services or meet any of its obligations under the CTP oversight regime. The regulators consider this to be sensible, and have caveated their rules accordingly.

Competition and unintended consequences

2.221 In CP26/23 the regulators proposed to prevent a CTP from using its designation as a badge of honour for marketing purposes. This was intended to mitigate the risk of firms misinterpreting a CTP's designation as a mark of regulatory approval, or as an indication that the CTP's services were inherently superior.

The halo effect and restrictions on CTPs' use of designation in marketing.

2.222 Most respondents who expressed a view were supportive of the regulators preventing a CTP from stating publicly that its designation by HMT somehow implied the endorsement of their regulators, or that its services were somehow superior to those of non-designated third parties providing similar services. There was some uncertainty among respondents regarding what exactly the proposed restrictions would prohibit. For instance, whether CTPs would be allowed to state publicly the fact that they were designated as CTPs.

2.223 Nine respondents were concerned that the proposed restrictions will not entirely prevent the impact of designation on competition in the market for third party services. Two main reasons were given for this view: (i) that the measure would be difficult to monitor and enforce in practice; and (ii) that, even with the proposed restriction in place, firms will likely perceive CTPs as more resilient than other third parties and gravitate towards them. In their consultation, the regulators referred to this potential perception as the 'halo effect' (see paragraph 11.10a of CP26/23).

2.224 Having considered the responses, the regulators have amended their rules and SS6/24 to clarify that the proposed restrictions do not prevent a CTP from making statements that explain, in a way that is fair, clear and not misleading:

- that the CTP has been designated by HMT;
- that the CTP is subject to oversight by the regulators in respect of systemic third party services it provides to firms; and
- the systemic third party services the CTP provides to firms.

2.225 The regulators have also amended the proposed requirement on a CTP to ensure that persons acting on its behalf do not contravene these restrictions with a requirement on the CTP to take reasonable steps to do so.

2.226 The fact that a CTP has been designated by HMT will be publicly known, as designation regulations will be public. What a CTP must not do, however, is imply that it has the approval or endorsement of the regulators by virtue of its designation by HMT, or that its designation confers any potential advantage to a firm or anyone else in using its services compared to a third party who is not designated as a CTP. These restrictions will be as enforceable as any other rules made by the regulators.

2.227 With regard to respondents' comments about the halo effect, the regulators highlight that the potential for such an effect may be offset by other impacts of the CTP oversight regime. For instance, a designated CTP will incur compliance costs due to being designated. Nine respondents noted that a CTP may pass these costs to its firm customers. These compliance costs may counterbalance any halo effect. Moreover, as the regulators have repeatedly stated in CP26/23, the SS6/24 and in this PS, firms 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. It follows that the regulators will continue to expect firms to justify the rationale for its choice of third party (whether or not a CTP) when entering into material third party arrangements. Simply stating that the firm choose a given third party above others by virtue of the fact that it was designated as a CTP without accompanying justifications is an insufficient explanation.

2.228 Having had regard to the responses, the regulators continue to consider it unlikely that the regime will significantly distort competition in the market in favour of CTPs.

The possibility of an opt-in mechanism

2.229 Four respondents who were concerned about a potential halo effect suggested that the regulators could mitigate any perceived competitive advantage that CTPs may gain by virtue of the regime by allowing third parties to voluntarily apply to be designated (referred to as

‘opting in’).

2.230 FSMA does not include an explicit opt-in mechanism for third parties wishing to be designated as CTPs. Designation decisions are a matter for HMT and a third party will need to satisfy the statutory test for designation under s312L of FSMA, whereby HMT may designate a person as a CTP ‘only if in [HM] Treasury’s opinion a failure in, or disruption to, the provision of those services (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system’. It is beyond the scope of the regulators' rule-making powers to create an opt-in mechanism as suggested.

The idea that the regime will put CTPs at a competitive disadvantage

2.231 Five respondents raised the opposite concern that the regime may put CTPs at a competitive disadvantage relative to non-CTPs, due to the additional costs and regulatory burdens incurred by CTPs. Seven respondents queried whether the regime might deter third parties from providing certain services to firms to avoid being designated.

2.232 Having regard for these views, the regulators continue to consider these risks to be very small and far outweighed by the Overall Objective. The regulators also highlight, as noted in the CP CBA, that many potential CTPs may already be preparing to comply with similar international regimes, and this may reduce the costs of compliance for CTPs with the UK regime insofar as it has commonalities with these international regimes. The proposals are compatible with non-UK initiatives such as DORA in the EU and the **Bank Service Company Act** (BSCA) in the US, which seek to fulfil similar objectives. Where they differ, they do not do so in a way that could reasonably be expected to detrimentally impact UK competitiveness and growth. The regulators therefore consider it unlikely that potential CTPs would withdraw or withhold services from the financial sector in order to avoid designation.

UK address for service

2.233 In CP26/23, the regulators proposed, in addition to the proposed requirement in Requirement 1 of the Operational Risk and Resilience Requirements to nominate a point of contact, a requirement for CTPs whose head office is outside the UK 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 proposed 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.

2.234 Respondents generally welcomed this proposal, and saw it as a sensible alternative to a stricter potential requirement for a CTP to set up an establishment (ie a branch or subsidiary) in the UK where one does not already exist. However, some respondents were

confused on the difference between these proposals and the abovementioned proposed requirement under Requirement 1 of the Operational Risk and Resilience Requirements. One respondent suggested that this requirement should either be deleted, or the regulators should clarify that a CTP could comply with it by meeting Requirement 1.

2.235 In response to this feedback, the regulators have further replaced this requirement with a clearer, simpler requirement that a CTP must provide the regulators with an address in the UK for the service of documents (including 'relevant documents' as defined in **The Financial Services and Markets Act 2000 (Service of Notices) Regulations 2001**). A CTP must also notify the regulators of any change to this information as soon as reasonably practicable.

2.236 These requirements apply to all CTPs (which is broader than the scope of the original proposal) but should not give rise to additional compliance burdens, and will prove particularly useful for those CTPs that are headquartered outside the UK, and do not have an establishment in the UK (ie a branch or subsidiary), as it ensures that the regulators can appropriately serve documents such as statutory notices to those CTPs.

2.237 For the avoidance of doubt, the requirement for an address for service applies in addition to Requirement 1.

Cost benefit analysis

2.238 In CP26/23, **Appendix 6: Cost benefit analysis** (the CBA) the regulators assessed the one-off and ongoing (annual) costs and benefits arising from the proposed policy. Based on the analysis of the costs and benefits of the proposals the regulators concluded that the proposals would bring net benefits to the UK financial sector. The proposals are proportionate due to the important role that CTPs are likely to play in affecting the system-wide resilience of the financial sector.

2.239 The CP included a question on the cost-benefit analysis, to which 28 of the total 62 CP respondents provided feedback.

Costs have been underestimated or are not captured

2.240 Twelve respondents claimed that the costs were underestimated. However, respondents did not provide supporting or alternative cost estimates. Other respondents argued that the CBA did not capture all potential costs to be incurred. The costs are discussed below.

Compliance costs to CTPs

2.241 Six respondents noted that costs to implement and comply with the regime, including new governance and reporting structures, maintaining a financial sector playbook, completing self-assessments, and the additional time required of senior accountable individuals, should be included in the CBA.

2.242 One respondent raised there would be additional costs resulting from updating contracts with firms outside the renewal period. Subsequent follow-up discussions with respondents indicated a cost of approximately £1 million in legal fees to update contracts.

2.243 One respondent suggested legal fees and remediation work resulting from any regulatory action taken should be included in the CBA while other respondents argued that, generally, costs in the CBA were underestimated.

2.244 In response, the regulators note that costs to CTPs to implement new governance and reporting structures, maintain a financial sector playbook, complete self-assessments, and time required from senior accountable individuals, are already captured within the cost categories set out in the CBA. The costings are based on a survey of third parties on the costs of implementing the proposals and estimates for large financial services firms on the costs to comply with the FCA's Operational Resilience regime for the financial sector.

2.245 The regulators further note that CTPs will be able to update contracts in line with their business as usual renewal cycle to avoid extra costs. This is in line with the proportionality elements of the regulators' 'have regards' analysis detailed within paragraph 11.13 of the CP, and preceding policy approaches. Therefore, there will be minimal costs from updating contracts with firms to take into account the new policy requirements.

2.246 The CBA assumes that CTPs will comply with the proposals as it is their legal duty to do so. Therefore, costs arising due to non-compliance are not included in the CBA.

Additional costs to firms

2.247 Nine respondents raised that there could be additional costs to firms arising from dealing with information requests from CTPs.

2.248 It is acknowledged within paragraph 51 to 52 of the CBA that, as customers of CTP services, firms may incur costs to familiarise themselves with the proposals. They will need to understand what information they can expect from CTPs that could help them to manage their operational resilience risks. This information will be integrated into their existing assurance work on third parties so these costs will likely be partially offset by current practices.

Competition impacts in the market for third party services

2.249 Six respondents raised that a market exit scenario should be reflected in the CBA. Twelve respondents raised that the regime may entrench concentration in the market as designation as a CTP could be seen as a superior level of recognition compared to other third party providers, suggesting there is a commercial advantage to being designated.

2.250 The potential impacts of the regime on the regulators' competition and innovation objectives are acknowledged within paragraphs 11.9 and 11.10 of CP26/23 and the competition impacts in paragraphs 90 to 97 of the CBA.

2.251 As noted in paragraph 90 of the CBA to address the risk of the proposed regime entrenching concentration in the market, the regulators proposed mitigations that included preventing a CTP using designation as a 'kite mark' of regulatory approval or endorsement, or that this confers any advantage to anyone using its services. Paragraphs 2.223 to 2.228 of this Policy Statement sets out the feedback received and how we have considered it.

2.252 In paragraph 93 of the CBA the regulators acknowledge the risk of CTPs exiting the market for services to the financial sector. The regulators have considered the feedback to the CP as set out in paragraphs 2.231 and 2.232. As noted in paragraph to 2.228 we consider it unlikely that the CTP regime will entrench further concentration on the basis that we have been clear about the meaning of designation. Additionally, there are a number of impacts (e.g. risk of enforcement action against the CTP, compliance costs) which may disincentivise firms from choosing a CTP over another third party. As many potential CTPs may already be preparing to comply with international regimes and since the costs are likely to be small relative to operating cost base of the types of providers that may be designated as CTPs, the regulators consider the risk of such impacts arising to be very small.

Monitoring effectiveness of the regime

2.253 Three respondents requested more detail on how the regulators would monitor the effectiveness of the regime.

2.254 Table 1 sets out the outcomes the regulators expect from the regime and the mechanisms through which we expect the regime to deliver these outcomes, as described in the causal chain in Figure 1 of the CBA analysis for CP26/23, and how the regulators will measure and monitor success.

Table 1: Monitoring effectiveness of the CTP regime

Reduced risk posed from concentrations of services to firms	Clear governance processes and roles that engage with the resilience of its systemic third party services, including approval and review of assurance provided to regulators	Concentrated services to firms are identified - monitoring concentration of services to firms provided by third parties using information from CTPs and firms Assessing the CTP's resilience to systemic risks via information gathered from regulators' oversight -The regulators' oversight of CTPs will assess the resilience of a CTP's systemic third party service based on compliance with the Operational Risk and Resilience Requirements; incident notifications; testing of CTP incident management playbooks (including lessons learned in self-assessment evidence shared with regulators); skilled person reviews; and engagement in sector-wide exercises.
Improved resilience of the wider financial system and economy	Identification of vulnerability and risks to systemic third party services across its supply chain and implemented appropriate controls	Firms see a reduction in the impact of CTP-related incidents – the regulators will monitor incident reporting data to identify issues with CTPs.
Better coordination across the financial sector where disruption originates at a CTP	Appropriate measure to manage the impacts of disruption to systemic third party services to firms, and to the stability of the UK financial system	Firms are better able to recover and respond to third party incidents within their impact tolerances - the regulators will monitor information on resilience shared by CTPs with their firm customers.
Reduced financial harm to firms and their customers	The ability to react and coordinate faster and more effectively to disruption, and so reduce the impact on firms	Firms are better informed of third party related risks - The regulators will assess the usefulness of the information sharing requirements through engagement with firms on improvements in their ability to management operational risk third parties pose.
Firms have continued access to systemic third party services	Improved coordination with firms and financial sector incident response framework if there is operational disruption	Impact of Operation Disruptions minimised for consumers, firms and markets - The regulators will monitor CTPs' responses to outages and disruptions from a range of sources, including gathering information from firms.

CBA conclusion

2.255 The concerns raised have been explored and discussed with stakeholders. Some elements which respondents highlighted, such as the costs of internal governance, are already covered within the cost categories set out in the CBA. Respondents did not provide alternative costings. Therefore, without new evidence, the regulators conclude that the costs set out in the CBA remain valid. If there is a slight increase in costs, the regulators consider the regime is still likely to be net beneficial as using conservative estimates of the potential benefits of the proposals, the estimated annual net benefits to the UK are between £5 million and £62 million. Additionally, major disruption at a CTP could result in significant costs. Three relevant incidents are a technology failure incident at the Royal Bank of Scotland in 2012, a major cyber incident at Tesco Personal Finance PLC in 2016, and a major incident at TSB Banking Group PLC in 2018. These incidents are estimated to have cost £158 million,[13] £22.7 million,[14] and £387.5 million[15] respectively.[16]

2.256 Following feedback to the CP, the regulators have made the following changes of note to the draft rules and guidance that are largely revisions that reduce the cost on CTPs. Therefore, the changes to the CP proposals do not alter the original CBA conclusion that the proposals would bring net benefits to the UK financial sector. These changes are:

- narrowing the scope of Fundamental Rules 1-5 and, reducing the incident reporting burden by narrowing the scope of a CTP operational incident and only requiring CTPs to submit intermediate incident reports where there's been a significant change in circumstances following an incident. These changes do not impact the regulators' ability to oversee the CTPs management of the services provided to firms and therefore fulfil the overall objective of the regime that relates to specific CTP services.
- providing additional guidance on some key concepts of the regime eg how a CTP impacts the stability of, or confidence in, the financial system, indicating what areas an incident management playbook should cover and, clarifying testing expectations. This additional guidance is likely to aid understanding of the role of CTPs in the financial system and therefore aid the management of the potential risks posed by CTP services to the financial system.
- enabling CTPs to use voluntary incident notification templates, to be shared in due course, that will enable the regulators to analyse the data more efficiently leading to faster identification of emerging risks. The information in the template will align with the policy the regulators consulted on and therefore, the change to the CP CBA would be costs relating to changing the format of submission which are likely to be minimal. As use of the template is voluntary, CTPs can decide to use an alternative approach (e.g. notifying via unstructured format such as email) to avoid incurring additional costs.

2.257 As such, following consideration of feedback and the impact of changes to the proposals, the regulators consider the CP CBA remains valid.

3: Enforcement

Bank of England and PRA enforcement

3.1 In March 2024, the Bank issued its consultation paper T**he Bank of England's approach to enforcement: proposed changes to statements of policy and procedure following the Financial Services and Markets Act 2023** ('Bank Enforcement CP'), which includes an annex on the Bank's approach to enforcement in respect of critical third parties. Feedback to this CP is provided in PS – **The Bank of England's approach to enforcement: changes to statements of policy and procedure following the Financial Services and Markets Act 2023**.

FCA enforcement

3.2 In Quarterly Consultation Paper (QCP24/3) the FCA consulted on proposed amendments to its Decision Procedure and Penalties Manual (DEPP) in the FCA Handbook to reflect proposed updates in relation to its enforcement policy with respect to critical third parties.

3.3 The following sections set out the FCA's feedback on the responses to the FCA's QCP24/3.

FCA summary of responses to FCA QCP24/3

3.4 The FCA received five responses to its proposals in QCP24/3. For completeness, the FCA has also reviewed and taken into account two additional responses shared by the Bank and PRA from the responses to the Bank Enforcement CP. The majority of the feedback was non-enforcement related. For the avoidance of doubt, the proposed amendments to DEPP sought to explain and invited responses on the policies the regulators would apply in exercising new or expanded enforcement powers. Those powers were conferred on the regulators by the Financial Services and Markets Act 2000 (as amended by the Financial Services and Markets Act 2023) and the scope of the enforcement powers was not the subject of the CP.

3.5 Respondents broadly welcomed the proposals, while raising some operational concerns and queries about practicalities. Some of these concerns, which did not directly relate to the regulators' approach on the use of enforcement powers, had already been expressed in response to the main consultation paper, jointly published by the Bank, the PRA and the FCA, on the overall regulatory oversight framework that will apply to CTPs: CP26/23 – **Operational**

resilience: Critical third parties to the UK financial sector. Feedback is provided in this chapter in relation to **FCA's Quarterly Consultation Paper No. 43** Feedback to responses to CP26/3 is addressed throughout this PS.

3.6 Respondents did not raise any Equality Act 2010 concerns.

FCA Feedback to responses to FCA QCP24/3

3.7 The FCA has considered the responses received to the QCP24/3. The FCA has decided to proceed with our approach to enforcement for CTPs as consulted on. In finalising our approach, we have taken account of the feedback to our proposals in QCP24/3.

3.8 This section summarises the responses under headings reflecting their subject matter and then sets out the FCA's feedback to those responses.

Responses and FCA feedback

Proportionate approach to enforcement

3.9 Three respondents stated that proportionality considerations around enforcement were essential (in deciding whether to investigate and in subsequently deciding whether to take enforcement action).

3.10 The FCA will consider all relevant factors ahead of taking any enforcement action to ensure any such action is proportionate. Proportionality is a requirement that applies across the FCA's regulatory scope and the FCA will take a consistent approach.

3.11 One respondent said it would be helpful if the FCA confirmed the types of evidence they will rely on when making enforcement decisions, including when evaluating the extent of the CTP's responsibility for a breach, and whether the FCA would consider, for instance, contracts between CTPs and their firm customers.

3.12 The FCA's use of its information gathering requirements will vary on a case-by-case basis. Whilst contractual requirements may form relevant context in a particular instance, the FCA's focus will be on determining whether or not a party has committed a regulatory breach. The new regulatory regime for CTPs does 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 from liability in any potential enforcement action.

Use of information gathering powers

3.13 Two respondents requested further clarity on how the FCA will exercise its information gathering powers, such as issuing statutory information requirements.

3.14 The FCA will consider how best to obtain relevant information to inform its regulatory approach and will exercise its powers accordingly on a case-by-case basis.

Use of condition or limitation powers

3.15 One respondent requested clarification as to the exact circumstances when the FCA will use their powers to impose conditions or limitations on the services provided by CTPs.

3.16 The FCA will consider the most appropriate disciplinary power, taking into account all relevant circumstances in each case. It is not possible to prescribe the exact circumstances in which the FCA would use any given power. The FCA will always act in a proportionate manner, taking into account all relevant considerations.

Confidentiality and information security

3.17 With respect to information sharing by the FCA during an enforcement investigation, three respondents raised concerns about confidentiality and information security.

3.18 The FCA acknowledges these concerns and agrees with the importance of maintaining confidentiality and strong information security. In addition to legal restrictions on the sharing of confidential information, to which it adheres, the FCA also employs strict information security controls. This will continue to be the case on any enforcement investigations relating to CTPs.

Unintended consequences of enforcement action

3.19 Five respondents stressed the importance of considering the risk that enforcement against CTPs (particularly where this involves prohibition) could have unintended, adverse consequences for firms and their end customers.

3.20 The FCA recognises that firms may face challenges obtaining services from an alternative CTP. The FCA will consider all relevant factors ahead of taking any enforcement action to ensure that any such action is measured. The FCA will consider the most appropriate disciplinary power, taking into account all relevant circumstances in each case.

Co-ordination between regulators

3.21 One respondent queried how the regulators will co-ordinate with each other to ensure clear alignment of approach in respect of enforcement against CTPs, given none of the three regulators is designated as the final arbiter.

3.22 Throughout the development of the CTP regime and this policy, the regulators have carefully considered this issue and agreed a new tripartite memorandum of understanding on how they will approach CTP oversight and enforcement. HMT has laid before Parliament the

regulators' **MoU** as required by s312V of FSMA.

Power to fine CTPs

3.23 Two respondents raised concerns about the lack of fining powers. The statutory powers, including enforcement powers, that the FSM Bill proposed to give the supervisory authorities in respect of CTPs were the subject of a **DP3/22** published in July 2022. FSMA does not provide the regulators with a power to impose a penalty on CTPs. As the extent of the powers is set out in FSMA, these were not consulted on in QCP24/3 and therefore are not within the remit of this PS.

---

1. **www.legislation.gov.uk/ukpga/2000/8/section/312L**
2. **www.legislation.gov.uk/ukpga/2023/29/contents**
3. As defined in s312P(10) of FSMA, and Section 2 of SS6/24.
4. **www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-impact-tolerances-for-important-business-services-ss**; **www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss** and **www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience**
5. Sections 138J(5) and 138K(4) of FSMA.
6. Whenever this PS introduces an amended or new term different to those in CP26/23, the rest of the PS uses the amended or new term.
7. Section 138J(2)(d) of FSMA.
8. CP26/23 Chapter 11: **www.bankofengland.co.uk/prudential-regulation/publication/2023/december/operational-resilience-critical-third-parties-to-the-uk-financial-sector**.
9. Sections 138I(3), 138I(4) and 138J(3), 138J(4) of FSMA.
10. Details on the regulators' approach to enforcement can be found in the regulators' respective SoP in Appendices 9 and 10 of this PS.
11. SS6/24 paragraph 6.32.
12. See the regulators' information-gathering powers over CTPs in s312P of FSMA extend to 'Persons Connected to a CTP', which include a CTP's internal auditors (even if employed by another entity in the CTP's group other than the designated entity or entities. See also section 4 in SS7/24 – Reports by skilled persons: Critical third parties.
13. RBS And Software Firm Settle Over IT Failure: **news.sky.com/story/rbs-and-software-firm-settle-over-it-failure-10381660**
14. FCA fines Tesco Bank £16.4m for failures in 2016 cyber-attack: **www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack**
15. TSB announces 2018 full year results: **www.tsb.co.uk/news-releases/tsb-announces-2018-full-year-results.html**
16. Shown in 2023 values.

Appendices

Appendix 1: List of respondents who have consented to the publication of their names (PDF)

Appendix 2: Bank of England FMI Rulebook: Critical third parties Instrument 2024

Appendix 2a: Bank of England FMI Rulebook: Critical third parties Emergency Provisions Instrument 2024

Appendix 3: PRA Rulebook: Critical third parties Instrument 2024 (PDF)

Appendix 4: FCA Handbook: Critical third parties Instrument 2024

Appendix 5: Supervisory statement (SS)6/24 – Operational resilience: Critical third parties to the UK financial sector

Appendix 6: Supervisory statement (SS)7/24 – Reports by skilled persons: Critical third parties

Appendix 7: The regulators' approach to the oversight of critical third parties

Appendix 8: The Bank of England's approach to enforcement: proposed changes to statements of policy and procedure following the Financial Services and Markets Act 2023 (the 'Enforcement PS')

Appendix 9: FCA Critical Third Parties Statement of Policy relating to Disciplinary Measures Instrument 2024

Other related publications

The proposed UK regime for critical third parties – speech by Gareth Truran

Critical Third Parties – HM Treasury's Approach to Designation

Memorandum of Understanding: between the Financial Conduct Authority and the Bank of England (exercising its prudential regulation functions)

Note: All content for this PS is included on this webpage. If you would like a PDF version of the PS, please use the button available below.