

# DP3/22 – Operational resilience: Critical third parties to the UK financial sector

PRA Discussion Paper 3/22 | FCA Discussion Paper 22/3

Published on 21 July 2022

## Content

### Foreword

---

#### 1: Introduction

- Definitions
- Discussion Paper Structure
- Responses and next steps

---

#### 2: The need for additional measures to manage the systemic risks posed by CTPs

- Implications of firms' and FMIs' increasing dependency on third parties
- Risks
- The evolving UK regulatory framework and CTPs
- Conclusion

---

#### 3: Introduction to the supervisory authorities' potential measures for CTPs

- Designation of CTPs
- Minimum resilience standards
- Resilience testing, participation in sector-wide exercises and skilled-persons reviews
- Alignment to the operational resilience framework for firms and FMIs
- Advantages of the potential future measures for CTPs
- Questions

---

#### 4: Identification of potential CTPs

- Initial considerations
- Potential factors to consider when assessing whether a third party meets the criteria for CTPs in the FSM Bill
- Combining the criteria
- Exemptions from designation

---

#### 5: Minimum resilience standards for CTPs

- Design features of the proposed resilience standards for CTPs
- Proposed minimum resilience standards for CTPs
- Identification and mapping
- Risk management
- Testing
- Engagement with the supervisory authorities
- Financial sector continuity playbook
- Post-incident communication plans
- Learning and evolving
- Interaction with recognised standards

---

---

**6: Resilience testing of CTPs**

Resilience testing tools  
Sector-wide exercises  
Cyber-resilience testing  
Information-gathering and skilled persons' reviews

---

**7: Supervisory authorities' use of proposed statutory powers over CTPs**

---

**8: International coordination and engagement**

8.5 The supervisory authorities are only able to introduce measures to advance their objectives. Therefore, the potential measures set out in this DP would be limited to the provision of services by CTPs to UK firms and FMIs as defined in Chapter 1. However, the supervisory authorities are mindful of the challenges posed by regulatory and supervisory fragmentation, and the corresponding need for ongoing international regulatory and supervisory alignment.

International initiatives relevant to CTPs  
Potential ways to improve international coordination on CTPs  
Questions

---

**9: Coordination with UK competent authorities and public bodies outside the finance sector**

Designation of CTPs  
Resilience Standards  
Testing  
Incident reporting  
Questions

---

**10: Questions**

---


**Annex 1: Academic, industry and international publications on CTPs**

Publications by UK public bodies  
Publications by international bodies  
Industry publications  
Academic publications

By responding to this discussion paper, you provide personal data to the Bank of England and the Financial Conduct Authority (FCA) ('we' or 'us'). This may include your name, contact details (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself.

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

The discussion paper will explain if responses will be shared with other organisations. If this is the case, the other organisation will also review the responses and may also contact you to clarify aspects of your response.

We will retain all responses for the period that is relevant to supporting ongoing regulatory policy developments and reviews. However, all personal data will be redacted from the responses within five years of receipt. To find out more about how the Bank deals with your personal data, your rights or to get in touch please visit [our privacy page](#). To find out more about how the FCA deals with your personal data please visit the [FCA's privacy page](#) .

Information provided in response to this paper, including personal information, may be subject to publication or disclosure to other parties in accordance with access to information regimes including under the Freedom of Information Act 2000 or data protection legislation, or as otherwise required by law or in discharge of the Bank's or FCA's functions.

Please indicate if you regard all, or some of, the information you provide as confidential. If we receive a request for disclosure of this information, we will take your indication(s) into account, but cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system on emails will not, of itself, be regarded as binding on us on us.

Responses are requested by Friday 23 December 2022.

**We prefer responses to be sent via email to:  [DP3\\_22@bankofengland.co.uk](mailto:DP3_22@bankofengland.co.uk).**

Alternatively, please address any comments or enquiries to:

The Recovery, Resolution and Resilience Team  
Prudential Regulation Authority  
20 Moorgate  
London  
EC2R 6DA


## Foreword

---

The UK financial sector is a complex, interconnected system in which financial services firms (firms) and financial market infrastructure firms (FMIs) increasingly rely upon third-party services to support their operations. Technology services such as cloud computing and data analytics can bring multiple benefits – enabling digital transformation, catalysing innovation, and providing greater resilience than firms’ and FMIs’ own technology infrastructure.

However, this increasing reliance on third parties also poses growing risks. In 2021, the Prudential Regulatory Authority (PRA), the Financial Conduct Authority (FCA) and the Bank of England (the Bank) (collectively the supervisory authorities) introduced new rules to strengthen firms’ and FMIs’ operational resilience. The supervisory authorities hold firms and FMIs responsible, and ultimately accountable, for their operational resilience, regardless of whether or not they rely upon third parties to support the delivery of their important business services.

But no single firm or FMI can adequately monitor or manage the systemic risks that certain third parties pose to the supervisory authorities’ objectives, including UK financial stability, market integrity and consumer protection. These systemic risks may arise when firms and FMIs rely upon a small number of third parties to provide services which, if disrupted, could significantly affect the authorities’ objectives (referred to as ‘material’ services in this discussion paper). For this reason, the Bank’s Financial Policy Committee (FPC) noted in 2021 that “additional policy measures, some requiring legislative change, are likely to be needed to mitigate the financial stability risks stemming from concentration in the provision of some third-party services”.

The relevant sections of the [Financial Services and Markets Bill](#)  (FSM Bill), which was put before Parliament on 20 July 2022, set out a proposed statutory framework for managing systemic risks posed by third parties designated as ‘critical third parties’ or ‘CTPs’ by HM Treasury (HMT). The supervisory authorities welcome the CTP proposals in the FSM Bill.

This discussion paper (DP) sets out how the supervisory authorities could use their proposed powers in the FSM Bill to assess and strengthen the resilience of services provided by CTPs to firms and FMIs, thereby reducing the risk of systemic disruption. The potential measures set out in this DP would focus on material services that CTPs provide to the financial sector. The supervisory authorities would not have any responsibility or powers for wider regulation and supervision of CTPs or for the resilience of the services they provide to other sectors. This service-based approach recognises that some potential CTPs may provide services to many other sectors besides financial services.

The potential measures set out in this DP comprise three main building blocks:

1. A framework for the supervisory authorities to identify potential CTPs and recommend them for

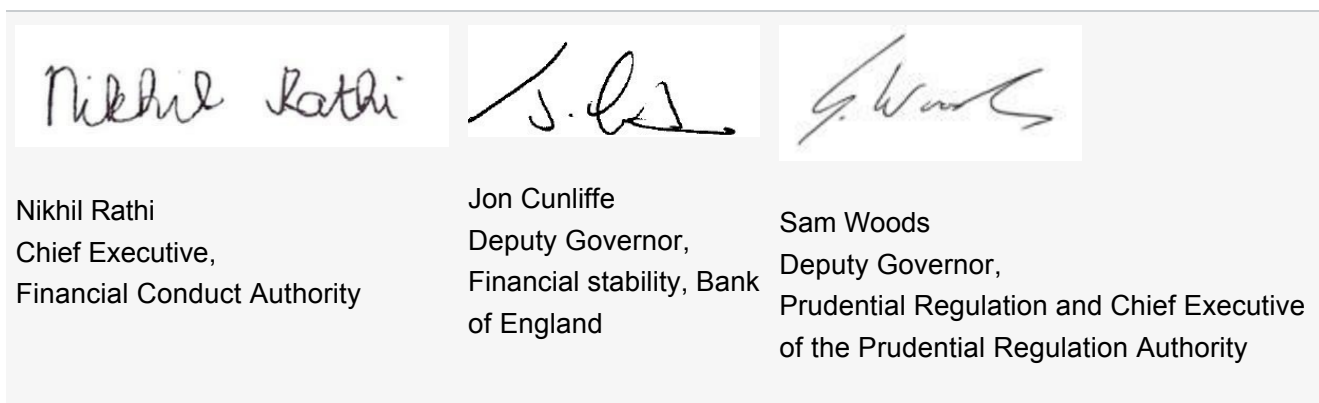
formal designation to HMT. CTP designation by HMT would recognise the potential systemic impact that disruption to the services provided by the third party could have on the supervisory authorities' objectives.

2. Minimum resilience standards for designated CTPs in respect of material services they provide to firms and FMIs. These standards would align to and build on the operational resilience framework for firms and FMIs, and would include a requirement for CTPs to develop and test 'financial sector continuity playbooks' to improve their ability to respond and recover from disruption affecting multiple firms and FMIs simultaneously.
3. A range of tools for testing the resilience of material services that CTPs provide to firms and FMIs. These tools could include, but not be limited to, scenario testing, participation in sector-wide exercises, cyber resilience testing, and skilled person's reviews of CTPs.

Core to the proposed approach would be the provision of information by CTPs to the supervisory authorities to assess the resilience of material services provided to firms and FMIs and address relevant concerns and issues. In addition, the FSM Bill proposes to give the supervisory authorities formal statutory powers (including enforcement) to achieve these outcomes, when appropriate and proportionate.

In all cases, these measures would seek to complement, but not replace, firms' and FMIs' own responsibilities to manage potential risks to their operational resilience, including as a result of the impact of the failure or disruption of a third party. The supervisory authorities also recognise that there could be unintended consequences stemming from the designation of CTPs, for example on competition, and would welcome industry feedback on ways to minimise these risks.

The systemic risks described above are not confined to the UK financial sector. Financial supervisory authorities in other jurisdictions, and UK regulators and public bodies responsible for other sectors face similar challenges. Mindful of the risks of regulatory fragmentation, and the desirability of interoperable approaches across jurisdictions and sectors, this DP sets out potential ways to improve international and cross-sectoral coordination in this area. Feedback to this DP will help shape a potential future CTP regime and inform the supervisory authorities' efforts to strengthen international and cross-sectoral co-ordination. The authorities anticipate consulting on the proposed measures once legislation receives Royal Assent. We strongly encourage stakeholders to share with us their views on the contents of this DP in order to help inform our work as it progresses.



## 1: Introduction

---

1.1 This discussion paper (DP) is issued jointly by the PRA, the FCA, and the Bank in its capacity as supervisor of FMIs (collectively the supervisory authorities).

1.2 The purpose of this DP is to share and obtain views on potential measures to manage the systemic risks to the supervisory authorities' objectives, including financial stability, market integrity and consumer protection, posed by certain third parties to the UK financial sector. These third parties, which would be designated by HMT via secondary legislation, are referred to as CTPs in this DP.

1.3 Implementing the potential measures discussed in this DP would require changes to UK legislation (in particular, the Financial Services and Markets Act 2000 (FSMA) and the Banking Act 2009). The Financial Services and Markets Bill (FSM Bill) contains the relevant proposed statutory measures. They include a framework for the designation of certain third parties as 'critical' by HMT; and new powers for the supervisory authorities to make rules for, gather information from, and take enforcement action against CTPs in respect of the services that they provide to firms and FMIs. This DP should be read alongside the relevant clauses in the version of the FSM Bill that was introduced to Parliament on 20 July 2022, and the '[Critical third parties to the finance sector: policy statement](#)' published by HMT on 8 June 2022. The potential measures in this DP are conditional on the relevant clauses in the FSM Bill being enacted in a substantially similar form.

1.4 Subject to the FSM Bill's passage, the supervisory authorities plan to consult on proposed rules and guidance for CTPs, based on their new statutory powers. Therefore, this DP refers to the measures that the supervisory authorities are considering introducing for CTPs as 'potential' to highlight that they may evolve and will be informed by responses to this DP.

1.5 The supervisory authorities' work in the area of operational resilience, including the potential measures examined in this DP, seeks to contribute to the UK Government's ambitions to ensure that the UK remains at the global cutting edge of technology and innovation in financial services. These ambitions were announced in the former Chancellor's [written statement](#) on the UK Government's response to the Kalifa Review of UK FinTech. The supervisory authorities' work also seeks to contribute to the resilience objectives in the the UK Government's [National Cyber Strategy 2022](#).

## **Box A: The supervisory authorities' objectives**

### **The Bank**

The Bank has an objective to protect and enhance the stability of the financial system of the UK. The Bank sets out in its Financial Stability Strategy that financial stability is the consistent supply of the vital services that the real economy demands from the financial system. Those vital services are:

- providing the main mechanism for paying for goods, services and financial assets;
- intermediating between savers and borrowers, and channelling savings into investment, via debt and equity instruments; and
- insuring against, and dispersing risk.

The Bank, as supervisor of FMIs, seeks to ensure that FMIs are designed and operated in a safe way, and that they contribute to reducing systemic risks in the vital payment, settlement and clearing arrangements centred upon them. The Bank's operation of the Real Time Gross Settlement (RTGS) service and CHAPS, the UK's high-value payment system, also supports the delivery of the Bank's overall mission.

### **The PRA**

The Financial Services and Markets Act 2000 (FSMA) defines the PRA's objectives, which are to:

- promote the safety and soundness of the firms it supervises; and
- contribute to the securing of an appropriate degree of protection for those who are or may become insurance policyholders.

The PRA also has a secondary competition objective.

### **The FCA**

The FCA's strategic objective is to ensure that relevant markets function well. To advance



its strategic objective, the FCA has three operational objectives:

- to secure an appropriate degree of protection for consumers;
- to protect and enhance the integrity of the UK financial system; and
- to promote effective competition in the interests of consumers.

In achieving their respective objectives, both the PRA and FCA seek to support financial stability.

## Definitions

1.6 This DP uses the following definitions, which should be interpreted consistently with those in the FSM Bill:

- firms include all firms authorised by the PRA and/or the FCA (both on a dual-regulated and FCA-solo regulated basis). The definition includes UK authorised branches of third-country firms;<sup>[1]</sup>
- FMI include central securities depositories (CSDs), central counterparties (CCPs), UK recognised investment exchanges, recognised payment systems operators (RPSOs), and specified service providers (SSPs) to RPSOs;<sup>[2]</sup>
- a ‘third party’ is ‘a person who provides services to one or more firms or FMIs’; and
- a CTP is a third party that HMT would designate as ‘critical’ using its proposed powers under the FSM Bill. Under the proposals in the Bill, HMT would be able to designate a third party as ‘critical’ if it was satisfied that a failure in, or disruption to, the provision of the services that the it provides to firms and FMIs (either individually or where more than one service is provided, taken together) could threaten the stability of, or confidence in, the financial system of the UK.

1.7 In this DP, the terms ‘disruption’ and ‘services’ should be interpreted broadly to include any disruption and services that are relevant to firms’ and FMIs’ operations. For instance, the processing of (personal and non-personal) data relevant to firms’ and FMIs’ operations, and the provision of facilities to firms and FMIs, are both considered a ‘service’ both in this DP and in the FSM Bill.

1.8 This DP is primarily relevant to third parties (in particular those that could be designated as CTPs by HMT under a potential future statutory framework), firms and FMIs. However, the supervisory authorities would welcome feedback from all stakeholders with expertise in relevant areas to this DP including but not limited to operational resilience, systemic risk, or third party risk management. The supervisory authorities would particularly welcome responses to the questions asked throughout the DP and listed in Chapter 10. Responses are requested by Friday 23 December 2022.

## Discussion Paper Structure

1.9 **Chapter 2** explores why the supervisory authorities consider it necessary to introduce additional measures to manage the systemic risks that CTPs pose to their objectives. In particular, it examines:

- the implications of firms' and FMIs' increasing reliance on third parties; and
- the evolving regulatory landscape.

1.10 **Chapter 3** introduces the supervisory authorities' potential measures for CTPs, which comprise:

- a framework for identifying potential CTPs and recommending their designation to HMT based on the proposed designation criteria in the FSM Bill;
- minimum resilience standards that CTPs could be required to meet in respect of certain services they provide to firms and FMIs (referred to as 'material' services in this DP); and
- resilience testing of CTPs set by the supervisory authorities using a range of tools, and focused on the 'material' services they provide to firms and FMIs.

1.11 **Chapter 3** explains that the supervisory authorities would not fully oversee, regulate or supervise CTP entities, or the services they provide to other sectors of the economy. Instead, the potential measures examined in this DP would focus on the services that CTPs provide to firms and FMIs. In particular, those services whose failure or disruption could have a systemic impact on the supervisory authorities' objectives (referred to as 'material' services in this DP). Chapter 3 also sets out why the supervisory authorities consider this potential approach as an effective, proportionate and targeted way to manage the systemic risks that CTPs pose to their objectives.

1.12 **Chapter 4** sets out the supervisory authorities' thoughts on a possible approach for identifying potential CTPs and recommending their designation to HMT. Under the FSM Bill, HMT would have the power to designate CTPs taking into account certain criteria. Designation would recognise the systemic impact that the disruption or failure of the services that a particular third party provides to firms and FMIs could have on the stability of, or confidence in the UK financial system. Before designating a third party as a CTP, HMT would consult the supervisory authorities, which, in practice, is likely to involve the supervisory authorities recommending the designation of a third party as a CTP to HMT. Against this background, Chapter 4 looks at how the supervisory authorities could:

- approach the high-level designation criteria for CTPs in the FSM Bill; and
- coordinate among themselves and, if appropriate, other UK competent authorities and public bodies outside the finance sector before recommending the designation of a third party as a CTP to HMT.

1.13 **Chapter 4** also highlights the supervisory authorities' intention not to recommend firms and FMIIs that they otherwise regulate or oversee for designation as CTPs provided that the supervisory authorities can obtain appropriate assurance about the resilience of any services that they provide to other firms and FMIIs via existing oversight or supervision.

1.14 **Chapter 5** sets out the supervisory authorities' thoughts on potential minimum resilience standards for CTPs. These potential standards would align to and build on the supervisory authorities' coordinated operational resilience framework for firms and FMIIs (summarised in the **Joint covering document 'Operational resilience: Impact tolerances for important business services'**), and focus on the ability of CTPs to prevent, adapt to, respond to, recover from, and learn from operational disruption. Under this approach, CTPs could be required to ensure that any material services that they provide to firms and FMIIs met the minimum resilience standards at all times. Firms and FMIIs would, however, remain accountable for managing risks to their individual operational resilience stemming from their arrangements with third parties.

1.15 **Chapter 6** outlines the supervisory authorities' potential approach to testing the resilience of material services that CTPs provide to firms and FMIIs using a range of tools, which could include but not be limited to scenario testing, participation in sector-wide exercises, cyber resilience testing, and skilled persons' reviews.

1.16 **Chapter 7** explains how the supervisory authorities could use the statutory powers that the FSM Bill proposes to grant to them in cases of actual or suspected non-compliance with applicable requirements by a CTP; to ensure that CTPs remediate outages or vulnerabilities; and to improve the resilience of the services they provide to firms and FMIIs.

1.17 In **Chapters 8 and 9**, the supervisory authorities discuss potential ways to improve coordination with non-UK financial supervisory authorities, international standard setting bodies, and relevant UK competent authorities and public bodies outside the finance sector given the cross-border and cross-sectoral nature of many CTPs, and of the services they provide.

**Annex 1** summarises recent publications, which have highlighted the systemic risks posed by CTPs, and informed some of the potential measures discussed in this DP.

## **Responses and next steps**

1.18 This DP closes on Friday 23 December 2022. The supervisory authorities invite feedback on the topics discussed in this DP. Please address any comments or enquiries to [DP3\\_22@bankofengland.co.uk](mailto:DP3_22@bankofengland.co.uk).

1.19 Subject to the outcome of Parliamentary debates on the FSM Bill, and after having considered responses to this DP, the supervisory authorities plan to consult on their proposed requirements and expectations for CTPs in 2023.

## 2: The need for additional measures to manage the systemic risks posed by CTPs

---

2.1 This chapter explores why the supervisory authorities consider it necessary to introduce additional measures to manage the systemic risks that CTPs pose to their objectives. In particular, the chapter discusses:

- the implications of firms' and FMIs' increasing reliance on third parties; and
- the evolving regulatory landscape.

### Implications of firms' and FMIs' increasing dependency on third parties

2.2 Firms and FMIs are becoming increasingly dependent on certain third parties for the delivery of functions and services that are vital to the stability of, or confidence in, the UK financial system. Cloud service providers (CSPs) are a frequently cited example of these third parties. However, there are other examples, including but not limited to other providers of information and communications technology (ICT) services, eg data analytics. The potential measures examined in this DP are technology-neutral and based on an assessment of the systemic risks that CTPs pose to the supervisory authorities' objectives.

### Benefits

2.3 The supervisory authorities recognise that well-managed outsourcing and other arrangements with third parties can bring benefits to firms and FMIs and, in some cases, to the supervisory authorities' objectives. These benefits include efficiency gains, reduced costs, scalability, faster innovation, better customer outcomes, and improved operational resilience.

2.4 For instance, the Bank's [response](#) to the Future of Finance Report noted that CSPs offer ready-made solutions that can reduce the time it takes for firms and FMIs to launch new products and services. With the benefit of their scale, they also offer leading-edge analytics, enabling businesses to learn and adjust their business models almost in real time.

2.5 ICT services offered by third parties, such as CSPs, can also be more resilient than individual firms' and FMIs' own ICT infrastructure, which often comprises legacy systems that rely on less up-to-date technology. CSPs also offer cybersecurity expertise, data storage and processing capabilities across a range of availability zones and geographic regions.<sup>[3]</sup> These features can enhance the ability of firms and FMIs to withstand and quickly recover from disruption.

2.6 The financial sector's response to the Covid-19 pandemic illustrated the advantages that third parties can bring to firms and FMIs. For instance, third parties providing a range of ICT services helped enable a fast and smooth transition to remote working. They also helped ensure that firms and FMIs could continue delivering essential services to customers and supporting the wider economy. A Bank of England Quarterly Bulletin article on '[The impact of Covid on machine learning and data science in UK banking](#)' published in Q4 2020 concluded that Covid-19 encouraged the use of outsourcing and third party providers by large banks.

2.7 Finally, the scalability and other features of some services offered by third parties, such as CSPs, can be more energy-efficient than individual firms' own infrastructure. Reliance on these services could help lessen firms' and FMIs' environmental impact, which could help advance the Bank's goal of 'ensuring the financial system is resilient to climate-related financial risks'. More information on the Bank's work on climate change can be found on its [climate change page](#).

## Risks

2.8 Notwithstanding the benefits highlighted above, the financial sector's increasing reliance on services provided by third parties also poses risks to individual firms and FMIs, to the supervisory authorities' objectives and to the wider financial system. These risks stem from a combination of:

- firms' and FMIs' growing dependency on third parties for services whose failure or disruption could have a systemic impact on the supervisory authorities' objectives (referred to as 'material' services in this DP);
- concentration in the provision of these services, which can arise from:
  - direct contractual arrangements between firms and FMIs, and third parties; and/or
  - indirectly through third parties' supply chains and other forms of interconnectedness.
- the potential impact of the failure or disruption of these services on the stability of, or market integrity of the UK financial system and the resilience of firms and FMIs. Factors such as the ability to recover or substitute a third party's services following disruption can in turn influence the potential impact that their failure or disruption could have.

2.9 Disruption to any material services that certain third parties provide to firms and FMIs could therefore lead to a single-point-of-failure [4]that may simultaneously impact:

- multiple firms and FMIs;
- these firms' and FMIs' counterparties, customers and/or direct participants (even if they do not directly rely on the relevant third parties' services); and
- in extreme cases, the financial stability of the UK.

2.10 In recent years, multiple publications by academia, industry and the public sector have highlighted the growing systemic risks posed by certain third parties to the financial services

sector. These publications, which are summarised in **Annex 1**, informed some of the potential measures discussed in this DP.




## The evolving UK regulatory framework and CTPs

2.11 The supervisory authorities' current powers allow them to impose requirements and set expectations on firms, FMIs, and certain parent undertakings. Since 2018, the supervisory authorities have used their existing powers to develop and implement a coordinated regulatory and supervisory framework to strengthen the operational resilience of the UK financial services sector (see the [joint covering document](#)). Operational resilience refers to the ability of firms, FMIs and the sector as a whole to prevent, adapt to, respond to, recover from, and learn from operational disruptions. The supervisory authorities have made clear that the operational resilience of firms and FMIs is a priority that should be viewed as no less important than their financial resilience. A lack of operational resilience represents a collective threat to the supervisory authorities' objectives, as well as their shared goal of maintaining financial stability. In particular, prolonged disruption to certain services and functions provided by firms and FMIs may impact the wider economy and UK financial stability.

2.12 The supervisory authorities' operational resilience framework requires firms and FMIs to:


- identify any services they provide to their external end users or clients that could impact the supervisory authorities' objectives if disrupted (known as important business services);
- set a tolerance for disruption for each important business service (known as an impact tolerance); and
- ensure they can continue to deliver their important business services and are able to remain within their impact tolerances during severe (or in the case of FMIs, extreme) but plausible scenarios.

2.13 Firms and FMIs are expected to be able to remain within the impact tolerances that they have set for their important business services even if they rely on third parties for the delivery of these services. The supervisory authorities have also taken steps in recent years to clarify, modernise, and strengthen their expectations on how firms and FMIs should manage their outsourcing and third party arrangements, by publishing:

- [FCA Finalised Guidance \(FG\) 16/5 'Guidance for firms outsourcing to the 'cloud' and other third-party IT services](#)  (which the FCA updated in 2019);
- their implementation of the [EBA Guidelines on outsourcing arrangements](#) , and [EBA Guidelines on ICT and security risk management](#); 
- [PRA Supervisory Statement \(SS\) 2/21 'Outsourcing and third party risk management](#); and
- The Bank's recent [CPs](#) on 'Outsourcing and third party risk management' for CCPs; CSDs,

RPSOs, and SSPs (as defined in page 8 of this DP).

2.14 These policy initiatives have helped to increase the focus on operational resilience within firms and FMIs, and encouraged a modernisation of their policies and processes for managing third party risks. They have also strengthened firms' and FMIs' ability to ensure that their contractual arrangements with third parties enable them to comply with their regulatory obligations. Nevertheless, there is widespread recognition that the existing financial regulatory and supervisory framework has inherent limitations when it comes to managing the potential systemic risks posed by CTPs. A key limitation is that no single firm or FMI can adequately monitor and manage risks stemming from concentration in the provision of services to multiple firms and FMIs by the same third party. Firms (including groups where applicable) and FMIs must manage risks to their own operational resilience. However, they cannot manage systemic risks that may arise because multiple firms and FMIs outside their group have independently decided to rely on a common third party for certain services. Several respondents to [PRA CP30/19 'Outsourcing and third party risk management'](#) highlighted this limitation and also noted an imbalance in negotiating power between firms and certain third party service providers. [PRA Policy Statement \(PS\) 7/21](#) summarises this feedback.

2.15 The supervisory authorities currently have some statutory information-gathering powers which can be exercised over service providers to firms. For instance, [Section 165A of FSMA](#)  gives the PRA what is known as the 'financial stability information power' (examined in Box B). However, the threshold for exercising this power is very high, and the PRA would need to complete a number of procedural steps each time it wanted to request information from a service provider. More importantly, this power does not extend to the other supervisory authorities and, even if it did, would not allow the supervisory authorities to implement most of the measures discussed in this DP, such as imposing minimum resilience standards on material services that CTPs provide to firms or FMIs, or require CTPs to take part in resilience tests.

### **Box B: The PRA's financial stability information power**

Under Section 165A of FSMA the PRA can require persons, including 'a service provider who provides any service to an authorised person' (which includes dual-regulated and FCA solo-regulated firms) and 'persons connected' to that service provider to provide specified information or documents that the PRA considers:

- are, or might be, relevant to one or more aspects of UK financial stability; and/or
- are reasonably required by the Bank in connection with the exercise of its functions in pursuance of its financial stability objective.

The PRA has issued a [Statement of Policy \(SoP\) 'The financial stability information](#)

**power**’ setting out how it intends to use its power under S165A of FSMA.

The PRA’s financial stability information power has inherent limitations that severely limit its usefulness as a potential tool to manage the systemic risks posed by CTPs. In particular:

- the PRA may use the power “only if [it] considers that— (a) the service or the way in which it (or any part of it) is provided, or (b) any failure to provide the service (or any part of it), poses, or would be likely to pose, a serious threat to the stability of the UK financial system”, which is a very high threshold;
- the power extends to service providers to dual-regulated and FCA-solo regulated firms only, but does not encompass service providers to FMIs;
- the power may be exercised only by the PRA, not by the FCA or the Bank acting other than as the PRA;
- the safeguards in s. 165B of FSMA make its regular and general use impracticable. These safeguards also indicate that the original policy intent was for this power to be used on an exceptional basis rather than as a means of obtaining regular assurance and information; and
- the power is limited to requiring the provision of information or documents and would not enable the supervisory authorities to implement the measures discussed in this DP.

The FSM Bill proposes to give the supervisory authorities a new power to gather information and documents from CTPs in a wider range of circumstances and with fewer procedural steps. The proposed power would, however, still be limited to information and documents reasonably required in connection with the exercise of the supervisory authorities’ proposed powers over CTPs. If this proposed information-gathering power over CTPs is implemented, Section 165A of FSMA would cease to apply to ‘service providers’ but would continue applying to the other persons mentioned in it.

2.16 The current regulatory framework limits the ability of the supervisory authorities to manage the systemic risks to their objectives posed by CTPs. Multiple, recent publications have highlighted these limitations, and have recommended the introduction of additional measures to strengthen the ability of the supervisory authorities to directly monitor and manage these risks (see Annex 1 to this DP).

### **The Financial Policy Committee’s focus on CTPs**

2.17 The Bank’s FPC has been monitoring the potential systemic risks posed by CTPs for several years. In the [June 2017 Financial Stability Report](#) (FSR), the FPC “requested annual updates from the financial authorities on the cyber resilience of firms that are outside the



regulatory perimeter, but which are important for the UK financial sector.”

2.18 In the **November 2018 FSR**, the FPC began closely monitoring CSPs after noting that, due to high concentration in the market for cloud services, “disruption at one provider, for example due to cyber-attack, could interfere with the provision of vital services by several firms.”

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

2.20 The FPC restated these views in the **Q3 2021** and **Q1 2022** FPS and Records. The former also described the “additional policy measures that were likely to be needed”, which this DP sets out in detail.

## **Treasury Select Committee Report on IT Failures in the Financial Services Sector**

2.21 The Treasury Select Committee’s 2019 **‘Report on IT failures in the Financial Services Sector’** [↗](#) (TSC IT Report), noted that:

- “Where the [supervisory authorities] identify that third-party providers are becoming a potential source of concentration risk, they should highlight this risk, and consider whether action is required to mitigate it. Where common providers are systemic, and concentration risk is high or becoming high, the [FPC] should in each case consider recommending to [HMT] that these should be regulated, as the [FPC] has done for FMIs.”
- “The consequences of a major operational incident at a large cloud service provider could be significant, and not just limited to the financial services sector. The case for the regulation of these providers to ensure high standards of operational resilience is therefore considerable. The Government should urgently consider how best to regulate cloud service providers.”

2.22 Some of the potential measures discussed in this DP build on ideas examined in the TSC’s IT Report. For instance, the report discussed “mandatory common standards for critical and common suppliers”, which they would have to meet and maintain ‘to supply financial services companies’ (see Chapter 5).

## **Kalifa Review**

2.23 In 2020, Ron Kalifa was commissioned by HMT to undertake a review of the UK Fintech Sector. Among other recommendations, the final **review** [↗](#) proposed:

- “an accreditation regime for unregulated service providers... whose support is essential for many financial institutions”; and
- “clear obligations for unregulated service providers’, such as ‘a direct obligation to comply with the outsourcing rules when they provide services to regulated financial institutions.”

## 2021 IMF UK FSAP Report

### 2.24 The IMF’s [2021 UK FSAP report](#) :

- noted that “cloud outsourcing heightens the need for more direct supervisory attention and understanding of the underlying structures and practices. In particular, firms’ increasing use of the cloud to perform core services raises operational (and potentially systemic) risks given the relatively small number of providers involved”; and
- recommended that the supervisory authorities seek additional statutory powers to review and examine the resilience of all critical services (including, but not limited to, cloud services) that third parties provide to regulated firms.

## Conclusion

2.25 The supervisory authorities recognise the potential benefits that services provided by third parties can bring to firms and FMIs and encourage the safe and sustainable use of these services. However, the failure of these third parties, or severe disruption to the material services that they provide could pose risks to individual firms, FMIs, consumers and, in some instances, the financial stability of the UK.

2.26 The current financial regulatory framework requires each firm and FMI to manage risks to their individual operational resilience, including where these risks stem from their reliance on third parties for the provision of important business services. The potential measures outlined in this paper would not alter these requirements on firms and FMIs. However, as multiple recent UK and international publications have highlighted, the current financial regulatory and supervisory framework has very limited tools to manage the systemic risks to the supervisory authorities’ objectives that could arise if the failure or disruption of certain third parties simultaneously impacted the provision of services to (a) one or more systemically significant firms or FMIs, or (b) multiple firms and FMIs. The supervisory authorities therefore consider that additional legislative and regulatory measures are needed, and therefore welcome the CTP proposals in the FSM Bill to allow the authorities to monitor and manage the risks posed by CTPs in an effective but proportionate manner.

## Questions

1. Do you agree with the supervisory authorities’ overview of the potential implications of firms’ and FMIs’ increasing reliance on third parties (in particular the potential systemic risks to the supervisory authorities’ objectives)? Is there anything else that the supervisory authorities

should consider in their analysis?

2. Do you agree with the supervisory authorities' assessment of the limitations of the current regulatory framework?

## 3: Introduction to the supervisory authorities' potential measures for CTPs

---

3.1 This chapter introduces the supervisory authorities' potential measures for CTPs, which Chapters 4-6 of this DP examine in detail:

- a framework for identifying potential CTPs which might be recommended for designation by HMT;
- minimum resilience standards for CTPs; and
- resilience testing of CTPs.

3.2 The supervisory authorities would not oversee, regulate or supervise CTP entities in their entirety, or the services they provide to other sectors of the economy. Instead, these potential measures would focus on those services that CTPs provide to firms and FMIs whose failure or disruption could have a systemic impact on the supervisory authorities' objectives (ie 'material' services, which are discussed in Chapter 4).

3.3 Firms and FMIs are accountable for managing risks to their operational resilience and will remain so under a potential future CTP regime, the purpose of which is to manage potential systemic risks stemming from the provision of material services to multiple firms or FMIs. The potential measures in this DP would therefore complement, but not replace, the responsibilities of individual firms and FMIs.

### Designation of CTPs

3.4 The FSM Bill proposes that HMT would have powers to designate certain third parties as CTPs, taking into account certain high-level criteria in the Bill, and following consultation with the supervisory authorities and other relevant bodies. The supervisory authorities might proactively recommend the designation of certain third parties as critical to HMT based on their analysis. The data and information needed for such analysis would come primarily from the supervisory authorities' supervision of firms and FMIs, but could draw on other sources (see Chapter 4).

3.5 The designation of a CTP by HMT would recognise the potential systemic impact that a disruption to its services could pose to the supervisory authorities' objectives, including financial stability, market integrity, or consumer protection. However, firms and FMIs would remain primarily

responsible, and ultimately accountable, for managing risks to their resilience arising from their arrangements with third parties, including but not limited to those designated as CTPs.

3.6 The FSM Bill proposes to give the supervisory authorities powers to make rules for, and gather information from designated CTPs in connection with the provision of services to firms and FMIs. The supervisory authorities are considering using these proposed powers to introduce minimum resilience standards for CTPs, and to require them to take part in a range of resilience tests and sector-wide exercises.

## **Minimum resilience standards**

3.7 The supervisory authorities' potential measures for CTPs could include rules setting out minimum resilience standards that CTPs would have to meet in respect of any material services they provide to firms and FMIs (see Chapter 5). The primary purpose of these resilience standards would be to mitigate the systemic risks to the supervisory authorities' objectives that could result from the failure of the CTP or a disruption to the services it provides to firms and FMIs. CTPs could demonstrate that they met the potential minimum resilience standards through:

- the provision of attestations and other relevant information to the supervisory authorities, eg the results of self-assessments;<sup>[5]</sup> and
- participation in the resilience tests and sector-wide exercises discussed in the next section and in Chapter 6.

## **Resilience testing, participation in sector-wide exercises and skilled-persons reviews**

3.8 The third element of the supervisory authorities' potential measures for CTPs could include rules requiring CTPs to carry out or take part in various resilience tests, which would focus primarily on the resilience of material services they provide to firms and FMIs. These tests could include, but would not be limited to, scenario testing, participation in sector-wide exercises and cyber resilience testing (see Chapter 6). Some of these tests and exercises could be carried out in collaboration with overseas financial supervisory authorities, or UK competent authorities and public bodies outside the financial services sector (see Chapters 8 and 9).

3.9 In addition to any potential future requirements to take part in resilience testing or sector-wide exercises, the FSM Bill proposes to give the supervisory authorities statutory powers to gather information directly from CTPs, and to commission skilled person reviews of CTPs.

## **Alignment to the operational resilience framework for firms and FMIs**

3.10 The supervisory authorities believe that an approach to CTPs focused on the two key elements set out above (minimum resilience standards and resilience testing) would align to and

build on their operational resilience framework for firms and FMIs, which has the following common features:

- **A focus on services:** The supervisory authorities' operational resilience framework requires firms and FMIs to focus on the resilience of the 'important business services' they provide. Likewise, the potential measures for CTPs would focus on the resilience of any 'material' services they provide to firms and FMIs.
- **The assumption that disruption would occur:** An assumption underpinning the supervisory authorities' operational resilience framework for firms and FMIs, and the potential measures for CTPs, is that disruption is inevitable. The potential measures discussed in this DP would not eliminate the risk of disruption. Their aim would be to assess and strengthen the ability of CTPs to prevent, adapt to, respond to, recover from, and learn from any disruption capable of having a systemic impact on the supervisory authorities' objectives.
- **Complementing firms' and FMIs' responsibilities:** A key principle underpinning the existing regulation and supervision of firms' and FMIs' outsourcing and third party arrangements is that boards and senior management, including (where applicable) individuals performing Senior Management Functions (SMFs), cannot outsource their responsibilities. Firms that enter into outsourcing and other arrangements with third parties remain fully accountable for meeting their regulatory obligations. The potential measures for CTPs examined in this DP would seek to strengthen the supervisory authorities' ability to monitor and manage the systemic risks that CTPs pose to their objectives, and which the existing regulatory and supervisory framework for firms and FMIs cannot fully manage at present. However, these potential measures would neither eliminate nor reduce the responsibilities of firms and FMIs and, where applicable, individuals performing SMFs for:
  - managing the risks in their material outsourcing and third party arrangements; and
  - taking appropriate measures to ensure that their important business services remain within their impact tolerances in case of severe but plausible disruption, including where they rely on a third party to support their delivery.

## Advantages of the potential future measures for CTPs

3.11 The supervisory authorities consider that their potential measures could be an effective and proportionate way to manage the systemic risks that CTPs pose to their objectives. In particular, the measures could have the following advantages:

- **Consistency with the existing operational resilience framework for firms and FMIs:** The potential measures for CTPs would build on the operational resilience framework for firms and FMIs. CTPs should already be familiar with this framework, which expects third parties to support firms and FMIs in their scenario testing, and the testing of their business continuity and exit plans for material outsourcing and third party arrangements.

- **A focus on services rather than the location of CTPs:** By focusing on the services that a CTP provides to firms and FMIs, the potential measures would be agnostic about the location of CTPs. This approach recognises that many CTPs provide services across international borders and/or to clients in multiple jurisdictions, and that this can help improve the efficiency and resilience of firms and FMIs. It could also reduce the potential compliance costs for CTPs, firms and FMIs compared to an approach that included a requirement for CTPs to localise entities, infrastructure, personnel or services in the UK.
- **Improved market discipline:** Requiring CTPs to ensure that any material services that they provide to firms and FMIs meet minimum resilience standards, and testing the resilience of these services could strengthen firms' and FMIs' ability (both individually and collectively) to oversee and obtain assurance from the CTPs they rely on. Some of the statutory powers that the FSM Bill proposes to give to the supervisory authorities over CTPs could also help strengthen market discipline (see Chapter 7).

## Questions

1. Do you agree that, when considering potential requirements for CTPs, it is appropriate for the supervisory authorities to focus on (a) minimum resilience standards, and (b) resilience testing, in respect of the material services that CTPs provide to firms and FMIs? Are there any alternative or additional areas that the supervisory authorities should consider?
2. Do you agree with the potential advantages in aligning the potential measures for CTPs to the existing operational resilience framework for firms and FMIs? Are there additional ways in which the potential approach to CTPs could be aligned to the existing operational resilience framework? Are there alternative approaches the supervisory authorities should consider?

## 4: Identification of potential CTPs

---

4.1 As proposed in the FSM Bill, HMT would designate certain third parties as CTPs via secondary legislation following consultation with the supervisory authorities. HMT would do so only if in its opinion a failure in, or disruption to, the provision of any services that those third parties provide to firms and FMIs (either individually or where more than one service is provided, taken together) could threaten the stability of, or confidence in, the financial system of the UK. The Bill proposes two high-level criteria that HMT would have to take into account when considering whether to designate a third party as a CTP:

- the materiality of the services the third party provides to the delivery by firms and FMIs (and, if applicable other persons on their behalf) of activities, services or operations (wherever carried out) that are essential to the economy of, or financial stability in, the United Kingdom (**materiality**); and

- the number and type of firms and FMIs to which the third party provides services (**concentration**).

4.2 In advising HMT on the designation of CTPs, the supervisory authorities would be likely to draw on their detailed analysis of relevant data and other evidence from their supervision of firms and FMIs (and other relevant sources). Against this background, this chapter focuses on:

- the factors that the supervisory authorities could take into account when assessing whether a third party may meet the high-level designation criteria for CTPs in the FSM Bill; and
- how the supervisory authorities could coordinate among themselves and, if appropriate, with relevant UK competent authorities and public bodies outside the finance sector before recommending the designation of a third party as a CTP to HMT.

## Initial considerations

4.3 CTPs are likely to comprise a very small percentage of the total number of third parties providing services to firms and FMIs. The proposed, high-level statutory designation criteria in the FSM Bill are deliberately designed to identify those third parties whose failure or disruption could have an impact on the supervisory authorities' objectives, including UK financial stability, market integrity and consumer protection. [6]

4.4 The supervisory authorities' approach to identifying potential CTPs, and recommending their designation to HMT, would be evidence-based. In practice, certain ICT third party service providers (such as the major CSPs) could be particularly likely to be considered for designation as CTPs due to firms' and FMIs' increasing reliance on their services. However, certain third party providers of non-ICT services, eg claims management services to insurers or cash distribution, could also be considered for designation as CTPs if they were deemed to meet the proposed statutory designation criteria.

4.5 As firms' and FMIs' reliance on certain services provided by third parties increases, supervisory authorities may identify new, potential CTPs. For instance, certain third parties providing data and artificial intelligence (AI) or machine learning (ML) models could emerge as future potential CTPs as a result of the increasing use of these data and models in trading systems, which could in turn lead to herding or procyclical behaviours (as noted in the final report of the [Artificial Intelligence Public-Private Forum](#)). Likewise concentration in the networks used to transfer data and AI/ML models could lead to the emergence of future CTPs given the potential for their disruption to pose risks to UK financial stability, market integrity or consumer protection. Moreover, as highlighted in a recent [paper](#) by the Financial Stability Institute (FSI) of the Bank for International Settlements (BSI) (summarised in **Annex 1**) "Big techs' investments in emerging technologies such as quantum computing are likely to deepen their critical role in the financial system. While this technology is at an early stage, it has huge promise." The FSI paper also noted that "experts envisage that few companies will be able to build or own quantum

computers in the near term and see a cloud computing-style model emerging where companies rent access to quantum machines hosted by a relatively small number of specialist providers”.

## Potential factors to consider when assessing whether a third party meets the criteria for CTPs in the FSM Bill

4.6 When considering whether to recommend a third party for designation as a CTP to HMT, the supervisory authorities could assess the materiality and level of concentration of the services it provides to firms and FMIs. The supervisory authorities could also consider the potential impact of the failure or disruption of those services (individually or if appropriate, taken together) on their objectives by looking at factors such as the substitutability of the services. Although the supervisory authorities might make recommendations, HMT would ultimately designate third parties as CTPs via secondary legislation.

### Materiality

4.7 A third party may provide a range of services to firms and FMIs of varying importance to the supervisory authorities’ objectives. The supervisory authorities could be more likely to recommend a third party for designation as a CTP to HMT where one or more of the services it provides to firms or FMIs was deemed ‘material’.

4.8 In assessing the materiality of the services that a third party provides to firms and FMIs, the supervisory authorities could take into account whether these services are critical to the delivery by firms and FMIs of:

- any of the economic functions listed in [PRA SS19/13 ‘Resolution planning’](#);
- ‘critical functions,’ as defined in [sections 3\(1\) and \(2\) of the Banking Act 2009](#) [↗](#); or
- certain ‘important business services’ as defined in the supervisory authorities’ operational resilience framework for firms and FMIs.

### Economic functions listed in PRA SS19/13

4.9 The list of economic functions in PRA SS19/13 (see Table A below) could be useful to assess whether the services that a third party provides to firms and FMIs might meet the materiality criterion in the FSM Bill. In particular, this list:

- already features in the supervisory authorities’ operational resilience framework for firms and FMIs. The supervisory authorities expect firms to take into account the potential for disruption to business services to inhibit the functioning of the wider economy, and in particular the economic functions in this list when identifying important business services (see [PRA SS1/21 ‘Operational resilience: Impact tolerances for important business services’](#) paragraph 2.5);



- has cross-border recognition. For instance, the European Systemic Risk Board (ESRB) report mentioned in **Annex 1** included a near-identical list of 'key economic functions of the financial system'.

**Table A: Economic functions listed in SS19/13**

Deposit taking and savings - which is also relevant to the FCA's objective to secure an appropriate degree of protection for consumers	Retail current accounts
	SME current accounts
	Retail savings accounts/time accounts
	SME savings accounts
	Corporate deposits
Lending and loan servicing	Retail mortgages
	Retail lending (secured/unsecured)
	Retail credit cards
	SME lending (secured)
	Corporate lending
	Trade finance
	Infrastructure lending
Credit Card Merchant Services	

Capital markets and investment	Derivatives
	Trading portfolio
	Asset management
	General insurance
	Life insurance, pensions, investment and annuities
Wholesale funding markets	Securities financing
	Securities lending
Payments, clearing, custody and settlement	Payment services
	Settlement services
	Cash services
	Custody services
	Third party operational services

## Critical functions / critical services

4.10 The supervisory authorities could also take into account whether the services that a third party provides to banks or banking groups were classed as '[critical services](#)' when assessing whether they met the materiality criterion.

4.11 The [Operational Continuity](#) part of the PRA Rulebook defines 'critical services' as those services that need to be available to one or more business units of a firm or entity of a group in order to provide 'critical functions' (as defined in [sections 3\(1\) and \(2\) of the Banking Act](#)

[2009](#) <sup>[7]</sup>).<sup>[7]</sup> By definition, the discontinuance of 'critical functions' is likely to lead to the disruption of essential services to the UK economy or to UK financial stability.

4.12 Firms in scope of the Operational Continuity part of the PRA Rulebook need to identify both their 'critical functions' and the 'critical services' needed to provide them. Their lists of these functions and services could be a useful reference point to help identify potential CTPs used by these firms.

### **(c) Important business services capable of having a systemic impact if disrupted**

69. The supervisory authorities could also take into account whether the services that a third party provides to firms and FMIs were critical to the delivery of certain 'important business services' in their operational resilience framework when assessing whether they met the materiality criterion.

4.13 As the supervisory authorities' joint covering document on '[Operational resilience: Impact tolerances for important business services](#)' clarifies, 'important business services' encompass "services that, if disrupted, would impact the supervisory authorities' objectives and thereby the public interest as represented by those objectives."

4.14 The supervisory authorities have not published a list or taxonomy of important business services. Firms and FMIs are responsible for identifying any important business services they provide and prioritising them.

4.15 Although disruption to all important business services beyond the impact tolerances that firms and FMIs assigned to them would, by definition, pose risks to one or more of the supervisory authorities' objectives, these risks may not always be systemic. However this could be the case for certain important business services. For instance, those:

- covered by an impact tolerance set by the FPC (eg payments) (see Q2 2021 FPS and Record paragraphs 67-82); or
- provided by FMIs, including but not necessarily limited to those mentioned in the following [Supervisory Statements](#):
  - Operational Resilience: Central Counterparties, paras. 2.3-2.6;
  - Operational Resilience: Securities Depositories, paras. 2.3-2.6
  - Operational Resilience: Recognised Payment System Operators and Specified Service Providers, paras. 2.3-2.5, 3.6-3.7.

4.16 As firms and FMIs refine their identification of important business services, the supervisory authorities could use this information to identify and specify other important business services which, if disrupted, could have a systemic impact on their objectives.

## Concentration

4.17 The supervisory authorities could also assess the level of concentration on a third party for the provision of services (in particular, material services) when considering whether to recommend that third party for designation as a CTP to HMT. Concentration in the provision of third party services to firms or FMIs is not inherently or invariably problematic. It can sometimes reflect the quality of a specific third party's services. However, concentration can, by definition, expand the number of firms and FMIs that could be simultaneously affected by the failure or disruption of a third party.

4.18 As highlighted in the [May 2022 Regulatory Initiatives Grid](#), the supervisory authorities intend to consult on a centralised framework for collecting "certain information on firms' outsourcing and third party arrangements in order to manage the risks they may present to the PRA/FCA's objectives, including resilience, concentration and competition risks". The outcome of this planned consultation could help ensure that recommendations by the supervisory authorities for HMT to designate certain third parties as CTPs were backed by relevant data. The planned consultation is also expected to include "clarity regarding the information firms should submit when operational incidents occur", which could likewise be relevant to CTPs. This project has been chosen as a phase two use case as part of the Transforming Data [Collection](#) Programme. The supervisory authorities expect to publish a CP on it in Q2 or Q3 2023.

4.19 The supervisory authorities could also look at other relevant sources of data, such as:

- firms' and FMIs' mapping of important business services;
- existing regulatory returns such as COREP 13 and [PRA 109](#), which include information on relevant firms' critical functions: or
- Notifications under the Senior Management Arrangements, Systems and Controls (SYSC) sourcebook of the FCA Handbook. In particular, [SYSC 8.1.12G](#) and [SYSC 13.9.2G](#) in the FCA Handbook, and Rule 2.3(1)(e) in the [Notifications](#) part of the PRA Rulebook.

4.20 When assessing concentration, the supervisory authorities may need to consider not just the number, but the type and significance of the firms and FMIs that rely on a given third party for material services. The failure of a third party, or a disruption to its services, could have a systemic impact on the supervisory authorities' objectives if it affected either:

- one or more significant firms or FMIs; or
- a large number of firms or FMIs even if they are not significant. These firms or FMIs could be of a specific type, or spread across the financial services sector.

4.21 An effective assessment of whether a third party met the concentration criterion in the FSM Bill would also need to capture:

- direct dependencies arising from contractual arrangements between firms and FMIs and third parties; and
- indirect dependencies which could arise (for instance) through supply chains and other forms of interconnectedness. Box C below provides an illustrative example of how direct dependencies and interconnectedness could materialise simultaneously.[8]

### **Box C: Illustrative example of direct dependencies and interconnectedness**

As part of firms' and FMIs' mapping of resources required to deliver their important business services under the supervisory authorities' operational resilience framework, consider a scenario in which eight banks and FMIs, all of which provide custody services to other firms, have identified three pieces of cloud-based software that all of them require to provide custody services.

A separate third party provides each piece of software. All three third parties rely on the same cloud service provider (CSP) for the infrastructure that supports their software. They are otherwise unrelated.

Five of the eight banks and FMIs also have a direct contractual arrangement with the same CSP for unrelated cloud services. The remaining three do not. In this scenario:

- all eight banks and FMIs have a direct dependency on each of the three software vendors.
- all eight banks and FMIs have (potentially unknown to them) an indirect dependency/interconnectedness on the CSP providing cloud infrastructure services to their three software providers.

Five of the eight banks and FMIs also have a separate, direct dependency on the same CSP, unrelated to their indirect dependency via their software providers.

4.22 The supervisory authorities consider that a potential way to help assess whether a third party met the concentration criterion in the FSM Bill could be to look at the combined market share of the firms and FMIs that rely on it for functions and services meeting the materiality criterion. If that combined market share exceeded a threshold set by the supervisory authorities, this could influence their judgement-based assessment of whether it meets the concentration criterion.

4.23 Table B illustrates how the supervisory authorities could assess concentration to identify potential CTPs using one of the economic functions listed in PRA SS19/13 (retail mortgages) as

an example. For illustrative purposes only, in this scenario, the example assumes that the supervisory authorities have estimated that disruption to 25% of UK retail mortgages could have a systemic impact. (No such assessment has yet been made.)

**Table B: Market share in UK retail mortgages**


1	Bank A	16%
2	Building Society A	13%
3	Bank B	11%
4	Bank C	11%
5	Bank D	9%
6	Bank E	8%
7	Building Society B	3%
8	Building Society C	3%
9	Bank F	2.5%
10	Building Society D	2%
11	Bank G	2%
12	Building Society E	2%
13	Bank H	2%
14	Building Society F	1.5%
15	Building Society G	1%

4.24 In this example, the supervisory authorities could hypothetically conclude that a third party meets the concentration criterion if its services were critical to the provision of retail mortgages by any combination of firms meeting the 25% threshold they had set. For instance:

- Bank A, which has the largest individual market share, plus any other firm in the top five;
- Building Society A and Bank B, which have the second and third largest market share respectively, plus any other firm on the list; or
- Firms ranging from Bank D to Bank F inclusive, which have the fifth to ninth largest market shares, etc.

4.25 As highlighted above, the 25% threshold in this example is purely for illustrative purposes, and is by no means an indication of where the supervisory authorities could set the concentration thresholds for UK retail mortgages. The objective of this example is to highlight the importance of taking into account not just the absolute number of firms and FMIs that depend on a third party, but also the relative significance of these firms and FMIs, when considering whether the third party meets the concentration criterion.

## Potential impact

4.26 The supervisory authorities could also look at the potential impact on their objectives of the disruption or failure of the third party or of its relevant services when considering whether to recommend it for designation as a CTP to HMT. Whereas materiality (discussed above) focuses on the importance of the services that a third party provides to firms or FMIs, potential impact focuses on features of the CTP and/or its services that could influence their potential to cause systemic risks to the supervisory authorities' objectives if they failed or were disrupted. For instance, such an assessment might consider how difficult the services might be to recover, restore or substitute. The idea of potential impact is baked into the definition of a CTP in the Bill. The concept, however, is neither new nor unique to CTPs. As the PRA's approach to **banking** and **insurance** supervision (collectively the PRA Approach Documents) explain, the PRA assigns a potential impact score to each dual-regulated firm based on its assessment of that firm's significance to the stability of the UK financial system. A firm's 'potential impact score' reflects its ability to "affect adversely the stability of the system by failing, coming under operational or financial stress, or because of the way in which it carries out its business." The highest category (Category 1) encompasses firms whose "size, interconnectedness, complexity, and business type give them the capacity to cause very significant disruption to the UK financial system (and through that to economic activity more widely) by failing, or by carrying on their business in an unsafe manner." The FCA also uses a 'Firm Assessment Model' (summarised in Annex 2 of the [FCA's Approach to Supervision](#) ) to assess potential harm to consumers and markets.

4.27 In assessing the potential impact of a third party's failure, or the disruption of any material services that it provides to firms and FMIs, the supervisory authorities believe it would be appropriate to consider whether such failure or disruption could threaten factors such as the:

- stability of the UK financial system, including through disruption to the operations of FMIs supervised by the Bank;
- continued delivery of key economic functions;
- safety and soundness of:
  - one or more systemically significant firms; or
  - multiple firms (whether systemically significant or not);
- market integrity and consumer harm; or
- likelihood of causing 'intolerable levels of harm' to large numbers of consumers.

4.28 Assessing the potential impact of the failure or disruption of a third party's services on the supervisory authorities' objectives is likely to involve an element of judgement. In exercising this judgement, the supervisory authorities could consider various factors, including but not limited to:

- the full range of services that the third party provides to firms or FMIs (known as aggregation risk);
- the substitutability of the services;
- potential ways for firms and FMIs to ensure the continuity or prompt recovery of these services if disrupted; and
- other relevant considerations, such as whether the third party (and other entities in its supply chain) have privileged access to firms' and FMIs' critical systems.

4.29 Firms and FMIs that rely on the services of a third party are best placed to assess the potential impact of its failure or a disruption to its services. The supervisory authorities' judgement of the potential impact of third parties' failure or disruption could therefore be heavily based on firms' and FMIs' assessments, including the results of their testing of:

- business continuity and exit plans for material outsourcing and third party arrangements; and
- severe but plausible scenarios (extreme but plausible scenarios in the case of FMIs) under the supervisory authorities' operational resilience framework for firms and FMIs.

### **Aggregation risk**

4.30 As noted above, the supervisory authorities could take into account the materiality of any services that a third party provides to firms or FMIs when considering whether to recommend it for designation as a CTP. However, in some situations, firms or FMIs may rely on the same third party for multiple services, each of which may or may not be material when considered individually. In certain circumstances, the cumulative impact of the failure of the third party or the





simultaneous disruption of most or all of the services it provides to firms or FMIs could also have a systemic impact on the supervisory authorities' objectives. This is referred to as 'aggregation risk', and is specifically considered in the FSM Bill, which notes that HMT may designate a third party as a CTP if the failure in, or disruption to, the provision of its services to firms or FMIs "either individually or where more than one service is provided, taken together, could threaten the stability of, or confidence in, the financial system of the United Kingdom."

4.31 A hypothetical example of aggregation risk could arise where a number of firms rely on the same third party for, say, both market data services and front office trading services. In this example, the potential impact of disruption to either of these individual services might not necessarily pose systemic risks to the supervisory authorities' objectives, but the simultaneous failure or disruption of both services might threaten confidence in the UK financial system. In considering whether to recommend such a third party for designation as a CTP to HMT, the supervisory authorities could take into account the aggregated risks described above.

## Substitutability

4.32 Multiple relevant publications identify a lack of substitutability of the services provided by third parties as a key potential cause of systemic risk. For instance:

- a 2017 report by the US Office of Financial Research entitled '[Cybersecurity and Financial Stability: Risks and Resilience](#)'  identified a lack of substitutability as one of "three channels through which cybersecurity events can affect financial stability" (the other two channels were a loss of confidence and a loss of data integrity); and
- A DP on '[Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships](#)'  published by the Financial Stability Board (FSB) in November 2020 (FSB DP) noted that "systemic risk could arise if, for instance, a sufficiently large number of FIs (or a single systemic FI) became dependent on one or a small number of outsourced or third party service providers for the provision of critical services that were impossible or very difficult to substitute effectively and in an appropriate timeframe, for instance due to limitations in the capacity of alternative third parties or other back-up solutions."

4.33 Although substitutability could be an important factor in assessing the potential impact of the failure or disruption of a third party's services, the supervisory authorities do not require firms and FMIs to adopt multi-vendor strategies. However, they recognise that these strategies can be part of a non-exhaustive menu of options to improve their resilience in certain circumstances (see [PRA SS2/21](#) para. 10.5).

## Survivability and other considerations

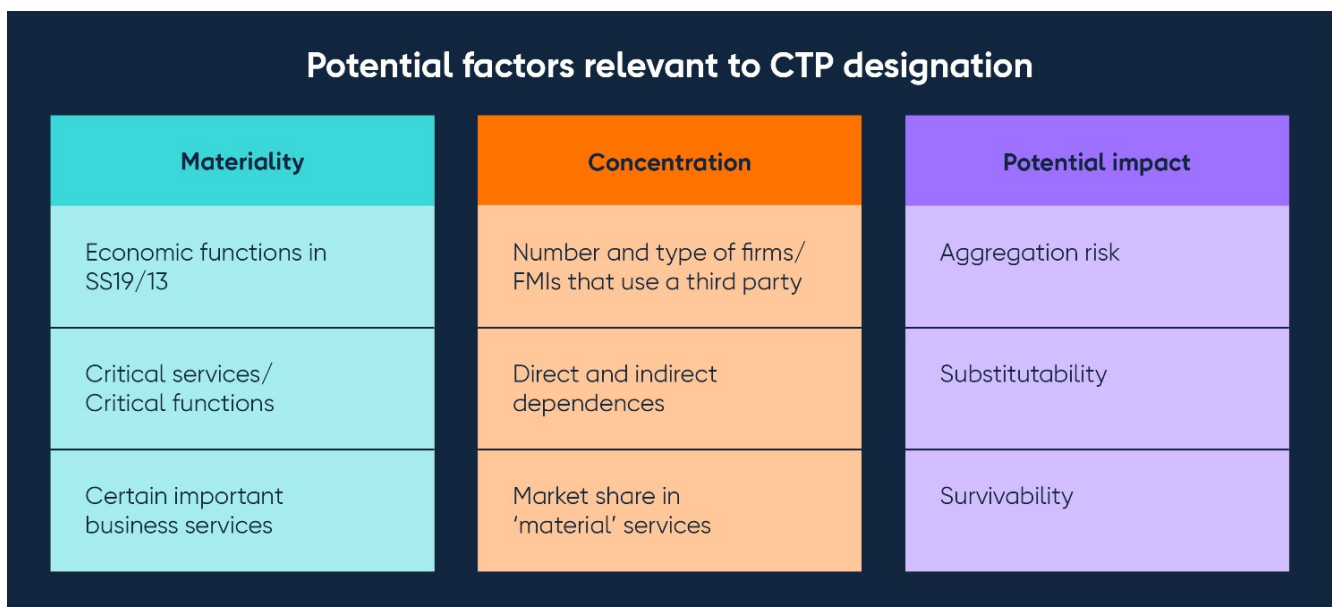
4.34 There might be available options to ensure the continued availability or timely recovery of a third party's services, which do not, strictly speaking, involve the substitution of a third party with

another (eg data vaulting). Some of these options might, however, be difficult for the supervisory authorities to assess in advance of designation. Where this is the case, survivability might, in practice, be more relevant to how the authorities assess whether a CTP has met the acceptable minimum standards of resilience rather than whether it met the criteria for designation.

4.35 The complexity and uniqueness of the services that a third party provides to firms and FMIs can also influence their survivability. For instance, if they involve intellectual property owned by the third party they might be harder to replicate or substitute. Likewise, the level of access to a firm’s important business services which a third party’s services could offer to a malicious attacker (which could, in some cases, be a current or former employee or subcontractor of the third party) could be another consideration. A related factor that could influence the potential impact of the disruption of a third party’s failure or disruption is the level of connectivity and access to firms’ and FMIs’ critical networks that it, and other entities and its supply chain, have.

### Combining the criteria

4.36 Figure B below, provides a visual summary of how the supervisory authorities’ could use these factors when considering whether to recommend a third party for designation as a CTP to HMT. Ultimately, HMT would be responsible for decisions on whether to designate certain third parties as CTPs, via secondary legislation.



### Governance and process of CTP designation recommendations

4.37 Although each supervisory authority would be able to recommend third parties for designation as CTPs to HMT, in most cases before doing so, it could consult the remaining supervisory authorities. In the case of dual-regulated firms and FMIs, the Bank, FCA and PRA could either issue joint recommendations for designation or seek the other authority’s agreement

before making recommendations to HMT individually as set out in a new or amended memorandum of understanding (MoU) between the supervisory authorities.

4.38 To promote cross-sectoral coordination, the supervisory authorities could also consider engaging with relevant UK competent authorities and public bodies outside the financial services sector before recommending certain third parties for designation as CTPs to HMT (in addition and without prejudice to HMT's separate proposed statutory duty in the FSM Bill to consult such other persons as it considers appropriate). These public bodies and competent authorities could include but not be limited to:

- the Department of Digital, Culture, Media and Sport (DCMS);
- members of the Digital Regulation Cooperation Forum (DRCF), including the Competition and Markets Authority (CMA) and the Information Commissioner's Office (ICO);
- the National Cyber Security Centre (NCSC);
- the Centre for the Protection of National Infrastructure (CPNI); and
- the UK Regulators Network (UKRN).

4.39 To facilitate this cross-sectoral dialogue, the supervisory authorities could explore potential communication channels with relevant UK competent authorities and public bodies outside the financial services sector.

4.40 The FSM Bill also proposes a separate requirement for HMT to have regard to representations from other relevant competent authorities and public bodies before formally designating a third party as a CTP.

4.41 The supervisory authorities could periodically review the circumstances and risk profile of a CTP and if relevant discuss the appropriateness of its continued designation with HMT.

4.42 Any recommendations that the supervisory authorities might make to HMT regarding the potential designation of a third party as a CTP would be based on an assessment of the systemic risks they may pose to the supervisory authorities' objectives. Nevertheless, the supervisory authorities are keen to minimise the risk of potential unintended consequences stemming from the designation of a CTP and the other potential measures in this DP. These unintended consequences could arise, if, for instance, firms and FMIs decided to only use designated CTPs for material services, which could inadvertently increase concentration and affect competition. The supervisory authorities would welcome feedback from respondents on possible ways to mitigate the risk of these potential unintended consequences.

## **Exemptions from designation**

4.43 A key objective of the potential measures for CTPs examined in this DP is to give the supervisory authorities a proportionate ability to oversee the provision of certain services to firms

and FMIs by third parties that are outside the financial regulatory perimeter, which, if disrupted, could pose systemic risks to their objectives.

4.44 Consequently, where firms and FMIs (and entities in their groups) are already subject to oversight, regulation or supervision by the supervisory authorities, such firms would not be recommended to be designated as CTPs provided that their existing authorisation(s), supervisory or oversight arrangements give the supervisory authorities the ability to impose equivalent requirements on the resilience of any services they provide to other firms and FMIs. These firms and FMIs could include:

- group service companies, whether regulated or unregulated on a solo basis;
- firms providing services to other firms outside their group, eg correspondent banking or custody; and
- FMIs.

4.45 Relevant equivalent requirements may include the:

- [PRA Fundamental Rules](#) [↗](#) / [FCA Principles for Businesses](#) [↗](#);
- Operational resilience framework for firms and FMIs; and/or
- Senior Managers and Certification Regime (SM&CR).

4.46 Subject to the outcome of a planned [HMT consultation](#) [↗](#), systemic payments firms and systemic payments-focussed service providers might, in future, be brought into the Bank's regulatory perimeter. Should this be the case, any systemic payments-related firms that may become subject to direct regulation and supervision by the Bank would also not be recommended for designation as CTPs.

4.47 However, there could be situations where a firm or FMI offers services to other firms or FMIs that:

- are deemed to meet the designation criteria for CTPs in the FSM Bill; and
- are not subject to oversight or supervision by the supervisory authorities under the firm's or FMI's UK authorisation or oversight arrangements.

4.48 A hypothetical example could be a service provided through a piece of software developed and sold by a division of a firm or FMI that is not regulated, overseen or supervised by any of the supervisory authorities. In this scenario, the proposed measures for CTPs could apply to that firm or FMI, but only in respect of the relevant service.

4.49 The Bank in its capacity as operator of RTGS/CHAPS would also be exempt from designation as a CTP. The Bank in its role as supervisor of FMIs supervises CHAPS on an arms' length, non-statutory basis in a similar way to other FMIs.

## Questions


1. What are your views on the factors that the supervisory authorities should consider when assessing which third parties to recommend for designation as CTPs? Are there any aspects of the criteria discussed above that the supervisory authorities should clarify, develop or omit? Are there any additional factors that the supervisory authorities should take into account?
2. What are your views on the supervisory authorities' potential approach for assessing concentration, materiality and potential impact in the provision of third party services to firms and FMIs? Are there alternative approaches for doing so that could be more effective or pragmatic?
3. What are your views on how best to take into account potential linkages with other regimes outside financial services when considering the recommendation of third parties as CTPs to HMT? How could the supervisory authorities improve coordination with other competent authorities and public bodies outside the finance sector?
4. What are your views on how best to avoid or mitigate potential unintended consequences, including potential distortion, such as deterring third parties from entering the market or providing services to firms and FMIs, as a result of a third party being designated as a CTP?

## 5: Minimum resilience standards for CTPs

---

5.1 This chapter sets out the supervisory authorities' thinking on a potential set of minimum resilience standards for CTPs in respect of the services they provide to firms and FMIs. These potential standards could align to and build on the operational resilience framework for firms and FMIs, and focus on the ability of CTPs to prevent, adapt to, respond to, recover from, and learn from operational disruption. Under this potential approach, CTPs would have to ensure that any material services they provide to firms and FMIs met the minimum resilience standards at all times.

5.2 The FSM Bill proposes to enable the supervisory authorities to make rules for CTPs. These rules would set out the resilience standards and associated requirements. To promote consistency and regulatory certainty, the FSM Bill proposes to require the supervisory authorities to coordinate the exercise of their proposed powers over CTPs, including their proposed rulemaking powers. In practice, this means that the supervisory authorities could issue coordinated sets of minimum resilience standards for CTPs. Any differences between the standards issued by the supervisory authorities would reflect their respective statutory objectives.

5.3 The current financial regulatory framework already includes global standards for critical service providers to FMIs. Annex F of the [CPMI-IOSCO Principles for FMIs](#)  sets out oversight expectations specifically targeted to service providers 'that are critical to an FMI's operations,

such as information technology and messaging providers'. The expectation in Annex F cover (a) risk identification and management; (b) information security; (c) reliability and resilience; (d) technology planning; and (e) communication with users. The expectations in Annex F are actively used in the supervision of critical service providers to FMI in the UK and globally. For instance, the Bank **requires** specified service providers to recognised payment system operators to have regard to Annex F, and submit an annual self-assessment against its expectations. The '**High Level Expectations for the Oversight of SWIFT**' [↗](#) are also modelled on Annex F.

5.4 The supervisory authorities consider that a set of standards similar to those in Annex F, but applicable and tailored to CTPs to the financial sector as a whole, could be a key tool for managing the systemic risks that they pose.

5.5 Although some of the potential minimum resilience standards for CTPs discussed below cover areas such as the identification, prevention and detection of incidents and risks, the assumption that 'from time to time, disruptions would occur' underpins the supervisory authorities' thinking on these potential standards.

5.6 CTPs could demonstrate compliance with the potential standards through the resilience tests and sector-wide exercises examined in Chapter 6, and regular (eg annual) attestations to the supervisory authorities. The supervisory authorities could also develop a rating system to assess CTPs' compliance with the potential minimum resilience standards, which could help promote clarity and consistency in their application. Examples of comparable, existing rating systems include the:

- Uniform Rating System for Information Technology (URSIT) used by the US Federal Financial Institutions Examination Council (FFIEC) to assess and rate IT-related risks of financial institutions and their technology service providers (see Appendix A of the FFIEC's **Supervision of Technology Service Providers booklet** [↗](#); and
- **NCSC's Cyber Assessment Framework** [↗](#) (CAF), which is used to assess the extent to which organisations are meeting a set of high-level cyber security and resilience principles, which are supported by contributing outcomes. Under the CAF, organisations are assessed as having 'achieved', 'not achieved' or (in some cases) 'partially achieved' each contributing outcome.<sup>[9]</sup>

## **Design features of the proposed resilience standards for CTPs**

5.7 The supervisory authorities consider that any potential minimum standards for CTPs should:

- apply to material services (see Chapter 4);
- build on the supervisory authorities' operational resilience framework for firms and FMIs;
- avoid duplicating existing, relevant standards;
- impose common, minimum obligations on CTPs; and

- be outcomes-focused and principles-based.

## Proposed minimum resilience standards for CTPs

5.8 Table C sets out the supervisory authorities' initial thinking on a potential set of minimum resilience standards that could be applied to CTPs. The rest of this chapter examines the potential standards in detail. Any such standards on CTPs would in due course need to be introduced by the supervisory authorities through their proposed rulemaking powers in the FSM Bill, and would need to be consulted on formally prior to introduction.

**Table C: Potential minimum resilience standards for CTPs**

1 Identification	The CTP has identified and documented all services that it provides to firms and FMIs, which, if disrupted, could have a systemic impact on the supervisory authorities' objectives (material services).
2 Mapping	The CTP has identified and documented the people processes, technology, facilities and information (collectively the resources) required for delivering its material services to firms and FMIs, including key nth parties and other key parts of its supply chain.
3 Risk management	The CTP has identified risks to its material services across its supply chain, and implemented appropriate controls.
4 Testing	The CTP regularly tests the resilience of its material services by <ul style="list-style-type: none"> <li>• participating in tests and sector-wide exercises convened by the supervisory authorities; and</li> <li>• performing its own tests.</li> </ul>
5 Engagement with the supervisory authorities	The CTP proactively and promptly discloses to the supervisory authorities any information of which they would reasonably expect notice. In particular, information relating to incidents or threats that could have a systemic impact on the supervisory authorities' objectives.
6 Financial sector continuity playbook	The CTP has developed and, to the extent appropriate, tested specific measures to address potential systemic risks to the supervisory authorities' objectives that could arise from its failure, or a severe but plausible disruption to its material services to firms and FMIs. The CTP has documented these measures in a 'Financial sector continuity playbook', which it regularly updates and submits to the supervisory authorities.

7 Post-incident communication The CTP has developed a tailored communication plan to engage with firms, FMIs, the supervisory authorities and other relevant stakeholders in the event of its failure, or a severe disruption to its material services. The communication plan should include proposed steps to manage the risk of a loss of confidence in the financial system linked to the CTP's failure or disruption. For instance, by including appropriate information about any measures that the CTP would take to recover or restore the material services, and the estimated timeframes for doing so.

8 Learning and evolving The CTP learns from any:

- severe disruption it experiences;
- known severe disruption at other relevant third parties;
- disruption at the firms and FMIs to which it provides services; and
- resilience tests and sector exercises that it performs or participates in. The CTP applies lessons learnt to the remediation of vulnerabilities, updates to existing services, and the development new services.

The CTP regularly shares these lessons with firms and FMIs and the supervisory authorities.

## Identification and mapping

5.9 Standard 1 could require CTPs to identify and document all material services they provide to firms and FMIs. In practice, CTPs may need to engage with the firms and FMIs they provide services to in order to accurately and fully identify these services.

5.10 Having identified the services, under Standard 2 CTPs could have to 'map' the necessary 'resources' to deliver them, including people, processes, technology, facilities and information. CTPs whose services rely on complex supply chains would have to ensure that their mapping captured the key 'nth parties' they rely on, and other key components of their supply chains. If applicable, CTPs could also identify any departments and individuals with specific responsibility for the delivery of relevant services to firms and FMIs (if applicable).

5.11 The concepts of 'identification' and 'mapping' derive from the supervisory authorities' operational resilience framework for firms and FMIs.

## Risk management

5.12 Standard 3 would cover the identification and prevention of risks to the CTP's financial and



operational resilience, including but not limited to:

- cyber risks;
- environmental risks, eg flooding and risks relating to climate change;
- risks to its financial viability as a going concern, such as the potential loss of a major customer or investor;
- geopolitical risks;
- legal and reputational risks; and
- 'insider risks' from their:
  - current and former employees (including contractors and employees in their main nth parties); and
  - key parts of their supply chain eg hardware, nth parties, premises etc.

## Testing

5.13 Chapter 6 below examines testing in detail.

## Engagement with the supervisory authorities

5.14 The supervisory authorities consider that a potential requirement on all CTPs to 'proactively and promptly disclose' to them 'any information of which they would reasonable expect notice' could be beneficial.

5.15 This potential requirement, which would be similar to PRA Fundamental Rule 7/ Principle 11 of the FCA Principles for Businesses, could focus on information relating to incidents or threats capable of impacting on the supervisory authorities' objectives.

5.16 As noted in Chapter 4, in parallel to this DP, the supervisory authorities are developing their approach to operational incident reporting by firms and FMI. Depending on how this future framework evolves, it could potentially also include requirements or expectations for CTPs.

5.17 As discussed in Chapter 9, the supervisory authorities would like to improve coordination with other UK competent authorities such as the ICO, which could facilitate the exchange of incident reports and other relevant information between the supervisory authorities and other UK competent authorities in different sectors.

## Financial sector continuity playbook

5.18 Standards 6-8 focus on CTPs' ability to respond to, recover and learn from severe but plausible disruption.

5.19 Standard 6 could require each CTP to develop, document, maintain and (to the extent

possible) test a 'financial sector continuity playbook'. These playbooks could set out the specific measures that a CTP would take to mitigate the potential systemic impact to the supervisory authorities' objectives of their failure, or severe disruption to any material services to firms and FMIs.

5.20 The supervisory authorities already expect firms and FMIs to develop, maintain and test individual business continuity plans and exit strategies for their material outsourcing and third party arrangements. Third parties are also expected to contractually commit "to take reasonable steps to support the testing of such plans"; and ensure that 'data owned by the firm can be accessed promptly in the case of the insolvency, resolution, or discontinuation of [their] business operations of the service provider' (see [PRA SS2/21](#) paragraph 6.4).

5.21 However, there are currently no direct requirements or expectations on third parties, including potential CTPs, to develop and test plans to manage the collective, simultaneous impact of their failure, or a severe disruption to their services on multiple firms or FMIs; the provision of services to the real economy; and/or the stability of, or confidence in, the UK financial system. A potential requirement for CTPs to develop, maintain and test financial sector continuity playbooks could address this gap, and promote greater coordination among CTPs, firms and FMIs that use their services and the supervisory authorities when responding to disruption.

5.22 In many cases, agreeing and implementing the measures in continuity playbooks could require cooperation between the CTP and other stakeholders. CTPs could therefore be expected to discuss, develop, test and (if necessary) implement their finance sector continuity playbooks in collaboration with:

- firms and FMIs that rely on their services, for example for the delivery of their important business services;
- industry bodies such as the Cross-Market Operational Resilience Group (CMORG);
- other relevant UK public bodies and competent authorities eg the NCSC; and
- if appropriate, other CTPs.

5.23 The supervisory authorities could also require CTPs to test their finance sector continuity playbooks appropriately and update them periodically.

5.24 The potential requirement for CTPs to produce finance sector continuity playbooks would be consistent with the PRA's revised operational continuity in resolution (OCIR) framework, which highlights similar playbooks as a possible tool for firms in scope of the Operational Continuity Part of the PRA Rulebook to demonstrate that they have "the capability to ensure continuity of critical services during possible changes to service provision resulting from restructuring related to recovery or resolution." Some firms are also expected to develop playbooks to support their recovery planning (see PRA [SS9/17 'Recovery Planning'](#)).

## Post-incident communication plans

5.25 A number of relevant publications, including the ESRB Report and OFR's report on systemic cyber risk mentioned in **Annex 1** and **Chapter 4** respectively, identify a loss of confidence in the financial system as a potential 'critical catalyst' that could turn an operational incident (specifically a cyber incident) into a source of financial instability.

5.26 The supervisory authorities therefore consider that a potential requirement for CTPs to develop and maintain post-incident communication plans to engage with relevant stakeholders, including firms and FMIs, following their failure or severe disruption could be important.

5.27 The primary purpose of these potential CTP post-incident communication plans, which could be part of their financial sector continuity playbooks, would be to mitigate the risk of an operational incident originating in or affecting a CTP becoming a systemic event due to, for instance:

- bank runs;
- liquidity shortages;
- market volatility;
- fraud and other crimes;
- mainstream and social media coverage (including misinformation); or
- other relevant amplification or transmission channels.

5.28 CTPs could be required to coordinate with relevant stakeholders in developing and, if necessary deploying, their post-incident communication plans.

## Learning and evolving

5.29 The purpose of all the potential measures discussed in this DP is to promote a continuous strengthening of the resilience of CTPs and the wider financial services sector.

5.30 Consequently, CTPs could be required to extract lessons learnt from (a) disruption including at their peers and customers; and (b) testing (see Chapter 6). CTPs could also be required to:

- apply these lessons to the remediation of vulnerabilities, updates to existing services, and the development of new services; and
- share them with firms, FMIs and their supervisory authorities to help strengthen their operational resilience and supervisory capabilities.

## Interaction with recognised standards

5.31 There are multiple government and industry-recognised certifications and standards (in particular in the area of ICT), which firms and FMIs can rely on for partial assurance about third

parties' control frameworks, including but not limited to the:

- NCSC's Cyber Essentials Plus and CAF;
- Germany's Cloud Computing Compliance Controls Catalogue (C5);
- The United States' FedRAMP certification;
- National Institute of Standards and Technology (NIST) Cybersecurity Framework;
- International Organization for Standardization's 2700x series;
- Center for Internet Security's Critical Security Controls; and
- Cloud Security Alliance's Cloud Controls Matrix.

5.32 The supervisory authorities wish to avoid unnecessary duplication between their potential resilience standards for CTPs and existing, relevant certification and standards. However, the latter often comprise checklists of controls, rather than demonstrable outcomes. Moreover, as many of these certifications and standards are cross-sectoral and focused on ICT security, they may not fully address all the risks to the supervisory authorities' objectives that CTPs may pose.

5.33 Consequently, the supervisory authorities may wish to take into account a CTP's compliance with relevant certifications and standards as partial or supporting evidence that it met their potential minimum resilience standards. However, such compliance would not automatically mean that the CTP demonstrably and fully met the supervisory authorities' potential resilience standards. This potential approach mirrors the supervisory authorities' expectations for how firms and FMIs should use these certifications and standards (see Chapter 8 of PRA [SS2/21](#)).

## Questions

1. Are the supervisory authorities' potential resilience standards for CTPs clear, comprehensive and proportionate? Are there any standards that the supervisory authorities could add, clarify, omit or review?
2. What relationship, if any, should recognised relevant certification and standards have with the supervisory authorities' possible minimum resilience standards for CTPs?
3. What are your views on the potential costs and benefits of complying with the minimum resilience standards discussed in this DP?

## 6: Resilience testing of CTPs

---

6.1 This chapter outlines the supervisory authorities' potential approach to testing the resilience of certain services that CTPs provide to firms and FMIs using a range of tools.

6.2 The supervisory authorities consider that a one-size-fits-all approach to CTP resilience

testing may not be effective, proportionate, or resource efficient. Therefore, they could rely on a range of resilience testing tools and sector-wide exercises, and periodically choose the most suitable for each CTP, taking into account the:

- number of material functions and services that the CTP's services support (see Chapter 4). For instance, a CTP whose services were considered essential to the delivery of multiple economic functions listed in SS19/13 would be likely to warrant more frequent and thorough testing than one whose services supported only one of those economic functions;
- type of services that the CTPs provides. Some testing tools, such as cyber resilience testing, may not be suitable for certain services;
- supervisory authorities' prior engagement with the CTP and knowledge about the resilience of the services it provides to firms and FMI, which may in turn depend on the CTPs' openness with the supervisory authorities;
- supervisory authorities' confidence about the resilience of the CTP's services. For instance, it could be appropriate to test a CTP with a history of disruption more frequently or rigorously;
- potential risk of disruption to the CTP's services as a result of testing; and
- cost, resource and time implications of the different testing tools on all parties involved.

6.3 The supervisory authorities would expect to carry out resilience testing of CTPs jointly where appropriate. For instance, where a CTP provides material services to both dual-regulated and FCA solo-regulated firms. At a minimum, the supervisory authorities would consult and coordinate with one another when considering whether to require a CTP to perform a specific test in line with their proposed obligation to do so in the FSM Bill.

6.4 Resilience tests and sector-wide exercises could, in principle, be performed jointly with non-UK financial supervisory authorities or relevant UK public bodies and competent authorities subject to appropriate cooperation arrangements being in place (see Chapters 8 and 9).

6.5 The supervisory authorities could also take into account the results of tests conducted:

- by the CTPs internally; or
- by or on behalf of:
  - non-UK financial supervisory authorities; or
  - UK competent authorities and public bodies, as long as these tests provide appropriate assurance about the resilience of their services to UK firms or FMI.

6.6 The supervisory authorities would need to develop ways to share the results of resilience tests on CTPs with, at least, those firms and FMI that rely on them for material services or are planning to do so in the future. In particular, the supervisory authorities would need to consider whether and how to bring any issues, risks and vulnerabilities identified during those tests, and any required or suggested remediation actions to the attention of relevant firms and FMI. In

doing so, the supervisory authorities would need to take into account potential confidentiality, market sensitivity and security considerations.

6.7 The supervisory authorities consider that resilience testing of CTPs could be an effective, proportionate and resource-efficient means to gain assurance over the likely resilience of CTPs' services to firms and FMIs for the following reasons:

- testing is a key element of the supervisory authorities' operational resilience framework for firms and FMIs. The supervisory authorities already expect third parties to support firms' and FMIs' testing of severe but plausible scenarios (extreme but plausible scenarios in the case of FMIs), and their business continuity and exit plans for material outsourcing and third party arrangements;
- testing would provide a direct, targeted way of assessing the resilience of certain services that CTPs provide to firms and FMIs; and
- all the potential forms of resilience testing discussed below could allow the supervisory authorities to leverage the expertise and resources of outside specialists or the CTPs themselves.

## Resilience testing tools

6.8 The rest of this chapter provides an overview of some of the potential resilience testing tools that the supervisory authorities could use with CTPs. However, this list is non-exhaustive. The supervisory authorities are particularly interested in suggestions for potential additional or alternative testing tools that could be appropriate for CTPs.

### Scenario testing

6.9 One of the most straightforward ways to test the resilience of any material services that CTPs provide to firms and FMIs could be for the supervisory authorities to introduce a requirement on CTPs to carry out regular scenario testing of their ability to continue providing these services in the event of their failure or severe but plausible disruption. Such a requirement could mirror the requirement in the supervisory authorities' operational resilience framework for firms and FMIs, but with appropriate modifications for CTPs.

6.10 Scenario testing could be the most frequently used testing tool due to its resource-effectiveness and versatility. In particular, it could be used to assess a number of aspects of a CTP's resilience.

6.11 Like firms and FMIs, CTPs could be expected to assume that disruption would occur, rather than taking comfort from an assessment of the relative probability of incidents occurring. The supervisory authorities would be particularly interested in CTPs' ability to prevent operational disruption from creating or amplifying systemic risks, including where:

- disruption originates at the CTP or its supply chain;
- the CTP itself becomes the cause of disruption due to, for instance, the actions of malicious insiders;
- disruption occurs as the result of the physical effects of climate change, for instance, flooding impacting data centres; or
- the CTP is a contagion or propagation channel for disruption originating elsewhere.

6.12 Under the supervisory authorities' operational resilience framework, firms and FMIs are required to identify severe but plausible scenarios to use in their scenario testing. The authorities could use the proposed rulemaking powers in the FSM Bill to issue similar requirements for CTPs. In addition, the supervisory authorities could require CTPs to test severe but plausible scenarios set by the supervisory authorities in collaboration with:

- firms, FMIs and industry groups, such as the Cross-Market Operational Resilience Group (CMORG);
- industry specialists, such as CBEST-accredited service providers (see Box D below for a description of CBEST);
- non-UK financial supervisory authorities; and/or
- relevant UK competent authorities and public bodies, such as the ICO.

6.13 The scenarios that CTPs could be required to test could draw on threat intelligence and previous disruption, including near misses (not necessarily confined to the UK or the finance sector) at CTPs, their customers, nth parties in their supply chain, and other CTPs providing similar services. Scenarios could also leverage firms' and FMIs' scenario testing under the supervisory authorities' operational resilience framework. This approach could allow the tailoring of scenarios to different CTPs.

6.14 Given the supervisory authorities' focus on potential systemic risks to their objectives, many scenarios (whether set by the supervisory authorities, or CTPs themselves) would be likely to involve multiple firms and FMIs simultaneously requiring the CTP to restore or support the continued provision of material services following disruption.

6.15 The supervisory authorities consider that it might be reasonable to expect CTPs' scenario testing to be at least as sophisticated as that performed by significant firms and FMIs. Where possible, any testing could include simulations or live systems testing, unless this could create an undue risk of disruption to the CTP's services. Desktop testing is ultimately unlikely to be sufficient for CTPs in most cases.

6.16. Although many scenarios are likely to involve disruption to firms' and FMIs' data stored or processed by a CTP, or to a CTP's ICT infrastructure or supply chain, the supervisory authorities' potential approach to testing could focus on all aspects of CTPs' resilience that could have a

systemic impact on the supervisory authorities' objectives. For instance, the physical effects of climate change could pose a threat to the stability of the wider financial system, and to the supervisory authorities' objectives. Consequently, the Bank's stress testing framework for banks and insurers includes climate scenarios under the **Climate Biennial Exploratory Scenario (CBES)**. Where relevant, CTPs could be required to consider similar climate scenarios in their scenario testing.

6.17. The financial resilience of some CTPs could also pose systemic risks to the supervisory authorities' objectives, particularly as some third parties could be designated as CTPs despite being relatively small in terms of financial metrics, such as revenue. In addition to operational disruption, these potential CTPs could be at heightened risk of financial failure, which could materialise quickly due to, for instance, the sudden loss of a major client or investor, or a spike in operating costs. Such financial failure could in turn give rise to step-in and other risks for firms and FMIs that depend on that CTP for material services.<sup>[10]</sup> Where this is the case, it could be appropriate for the supervisory authorities to focus on the financial, as well as the operational resilience of those insofar as it may impact the services CTPs provide to firms and FMIs. This could involve asking CTPs to consider scenarios relating to their financial resilience, and to provide evidence of any measures they have in place to ensure the continued provision and orderly transfer of material services to firms and FMIs in the event of their financial distress or failure, eg administration and other insolvency proceedings. The focus of the supervisory authorities would be on the potential implications of the CTP's financial distress or failure on the continuity of any material services it provides to firms and FMIs (or the ability to transfer those services). The supervisory authorities would not be responsible for setting specific standards of financial resilience for CTPs in the same way they do for firms and FMIs.

## Sector-wide exercises

6.18 Unlike other potential tools examined in this chapter, which would test the resilience of individual CTPs, sector-wide exercises are designed to validate the ability of the financial services sector as a whole to respond to severe but plausible sector-wide operational incidents.

6.19. Sector-wide exercises involve multiple firms and FMIs and can be led by financial supervisory authorities or industry bodies.

6.20 Examples of sector-wide exercises in the finance sector include:

- FPC cyber stress tests;
- Sector Simulation Exercises (SIMEX) carried out by the Cross Market Business Continuity Group (CMBCG) a key coordination group of the UK finance sector, the supervisory authorities and HMT;<sup>[11]</sup> and
- the '**Quantum Dawn** [↗](#)' series, which is industry-led but includes participation by financial supervisory authorities in several jurisdictions.



6.21 Sector-wide exercises can provide valuable lessons for the entire finance sector. As highlighted in the 2021 speech [Cyber Risk: 2015 to 2027 and the Penrose steps](#) by Lyndon Nelson (former Deputy CEO of the PRA and Executive Director, Regulatory Operations and Supervisory Risk Specialists), these exercises:

- “build capabilities internally and across the sector. They provide an opportunity to rehearse assigned roles and responsibilities and build the muscle memory such that reactions become instinctive and measured. They provide a safe environment to prepare for known threats, play out scenarios in ‘slow time’ and identify weaknesses which a crisis might otherwise expose. Exercises can also be used to demonstrate or validate response capabilities, with a focus on managing the impacts regardless of cause.”

6.22 As Chapter 8 examines, an additional benefit of sector-wide exercises is that they can be, and previously have been, carried out on a cross-border basis in collaboration with non-UK financial supervisory authorities.

6.23 Requiring CTPs to participate in sector-wide exercises could be a helpful way to assess and strengthen the resilience of the entire financial services ecosystem. For instance, a scenario involving severe disruption to a CTP’s services to multiple firms and FMIs could help improve the individual and combined response and recovery capabilities of that CTP, firms and FMIs that use its services, the supervisory authorities and bodies such as the NCSC.

6.24 The main drawback of sector-wide exercises is the level of coordination, resources and time required to organise them, which explains why the exercises referred to above take place approximately every two to three years. The supervisory authorities could therefore expect to use sector-wide exercises in conjunction with other testing tools that can be used more frequently, such as scenario testing.

## Cyber-resilience testing

6.25 Another tool that the supervisory authorities could use to test certain CTPs is cyber-resilience testing. As Box D explains, cyber-resilience testing of firms and FMIs is a well-established tool in the UK.

### **Box D: The current UK cyber resilience testing framework for firms and FMIs**

CBEST, which is a threat intelligence-led penetration testing framework, is the supervisory authorities’ flagship testing programme for cyber resilience.

The latest version of the [CBEST Implementation Guide](#) explains that CBEST ‘promotes

an intelligence-led penetration testing approach that mimics the actions of cyber attackers intent on compromising an organisation's important business services and disrupting the technology assets, people and processes supporting those services.' CBEST's intelligence-led approach is one of its differentiating characteristics.

At present, CBEST testing focuses on a 'core group' of systemically significant firms and FMIs which the supervisory authorities review every three years. CBEST focuses on these firms and FMIs security controls and capabilities when faced with a simulated cyber-attack. The simulated attacks used in testing are tailored to the threat and vulnerability profile of each organisation and represent an evidence-based and robust testing approach.

At the end of each CBEST test, each participating firm/FMI agrees a remediation plan with its supervisor to address identified vulnerabilities. These remediation plans are the primary focus for addressing the participant's cyber-resilience issues.

The supervisory authorities also publish regular thematic feedback that can be incorporated in participating firms' and FMIs' remediation plans. The latest [thematic findings](#) were published in 2021.

The CBEST framework is constantly evolving and recognises firms' and FMIs' growing reliance on third parties. The current CBEST Implementation Guide notes that "supply chain scenarios ...should always be analysed and discussed during CBEST", and recommends that firms and FMIs 'plan in advance the involvement of staff and third parties to increase the reality of assessment."

In addition to CBEST, the supervisory authorities have developed a scaled-down threat intelligence-led penetration testing framework known as STAR-FS. A key difference between CBEST and STAR-FS is the considerably reduced role of the supervisory authorities in the latter, which makes it accessible to a wider range of firms, as well as more resource-efficient.

6.26 Conducting cyber-resilience testing of certain CTPs could be a useful tool. However, this testing may need to be tailored to different types of CTPs to be effective. Some potentially, non-mutually exclusive, ways to carry out cyber-resilience testing of CTPs could include:

- individual cyber-resilience testing of a selected group of CTPs (similar to the 'core group' of firms and FMIs under CBEST) overseen by the supervisory authorities on a rotating basis (eg each CTP in the group could be tested every three years);
- a wider range of CTPs performing their own cyber-resilience testing with limited oversight from the supervisory authorities. These CTPs could be required to share the results of these tests

with the supervisory authorities, and agree a remediation plan; and/or

- a requirement for relevant CTPs to actively support the cyber resilience tests of firms and FMIs ie CBEST or STAR-FS.

6.27 Cyber-resilience testing has certain limitations, which mean that it could not be used as frequently as scenario testing. For instance, it is resource-intensive (an individual CBEST assessment takes approximately nine months to complete). Moreover, cyber-resilience testing of certain CTPs, such as CSPs, would need to take into account the complexity of their ICT infrastructure, and the fact they provide services to institutions in multiple sectors. Consequently, cyber-resilience testing could require the active collaboration of CTPs. These issues could influence how these cyber-resilience tests could be scoped and performed (and by whom).

## Information-gathering and skilled persons' reviews

6.28 The FSM Bill proposes to grant the supervisory authorities the power to gather information directly from CTPs. The supervisory authorities would be able to do this by requesting relevant information or documents directly from CTPs, and by commissioning skilled persons' reviews of CTPs (akin to their powers under Sections [166 of FSMA](#) [↗](#) and [195 of the Banking Act 2009](#) [↗](#)). Skilled persons' reviews could be used for a variety of purposes, including resilience testing.

6.29 The FSM Bill would place a statutory obligation on CTPs to give skilled persons all such assistance as they may reasonably require. This obligation would extend to any person who is providing (or who has at any time provided) services to the CTP concerned in relation to the matter concerned, including 'nth parties' in a CTP's supply chain.

6.30 Unlike other resilience testing tools, which could be used cyclically or regularly, the supervisory authorities could use skilled persons' reviews of CTPs more selectively. For instance, if they had specific concerns about an aspect of the services that a CTP provides to firms or FMIs, or to monitor the implementation of actions they had requested the CTP to take eg in response to an incident (see Chapter 7). As with firms and FMIs, the supervisory authorities could either appoint skilled persons directly from a panel, or approve a skilled person nominated by a CTP.

## Questions

1. What are your views on the potential resilience testing tools for CTPs discussed in this chapter? Are there any additional or alternative tools that the supervisory authorities could consider applying to CTPs?
2. How could the supervisory authorities work with CTPs, firms and FMIs and other stakeholders to make resilience testing of CTPs efficient, proportionate and resource-effective?
3. In terms of the different potential forms of cyber-resilience testing discussed in this chapter, are there any that could be particularly effective for CTPs? Conversely, are there any that could be

particularly difficult to implement in practice or give rise to unintended consequences?

4. What do you think could be the most effective way for the supervisory authorities to share the findings and recommended actions of any resilience testing performed by or on CTPs with, at least, those firms and FMIs that rely on them for material services? How could the supervisory authorities balance the need to share this information with relevant firms and FMIs with potential confidentiality or market sensitivity considerations? Could a rating system along the lines of the URSIT system used by the FFIEC in the US promote clarity and consistency in supervisory authorities' assessments?

## 7: Supervisory authorities' use of proposed statutory powers over CTPs

---

7.1 This chapter summarises the statutory powers, including enforcement powers, that the FSM Bill proposes to give the supervisory authorities in respect of CTPs.

7.2 The overriding goal of the measures discussed in this DP is to manage the systemic risks that CTPs pose to the supervisory authorities' objectives. Therefore, the supervisory authorities envisage using dialogue with CTPs to obtain relevant information, assess the resilience of their services to firms and FMIs, and address relevant concerns and issues. The supervisory authorities may also ask firms and FMIs (through their business-as-usual supervisory interaction) to enhance their due diligence, monitoring or business continuity, and exit plans for any material services they receive (or plan to receive) from a specific CTP, if they have concerns about its resilience. The supervisory authorities could also consult on requirements on CTPs to share information with firms and FMIs that use their services relating to regulatory concerns and recommended remediation.

7.3 In addition, the FSM Bill proposes to give the supervisory authorities formal statutory powers to achieve these outcomes, which will be used if appropriate and proportionate. The supervisory authorities could use these powers if:

- they deem it necessary or expedient to advance their objectives; or
- there are circumstances suggesting that a CTP may have breached an applicable requirement.

7.4 These proposed powers include:

- issuing a direction requiring a CTP to do, or refrain from doing, anything specified therein, eg:
  - implementing the recommendations of a review conducted by a skilled person or other

independent party;

- remediating issues or vulnerabilities identified in resilience tests, sector-wide exercises, or actual disruption; or
- suspending or imposing conditions or restrictions on the CTP's ability to provide services to firms and FMIs;
- appointing a skilled person to provide a report on the CTP's compliance with relevant requirements. Such a report could be used, among other purposes, to assess the CTP's implementation of actions set out in a direction;
- if a CTP breaches an applicable requirement:
  - publishing a statement (censure) with details of the CTP's breach;
  - imposing conditions or limitations on the ability of the CTP to provide services to firms and FMIs;
  - issuing a disqualification notice to the CTP:
    - prohibiting it from entering into future agreements with firms and FMIs for the provision services, and prohibiting firms and/or FMIs from such an agreement with a CTP;
    - prohibiting it from continuing to provide some or all services to firms and/or FMIs, and prohibiting firms and/or FMIs from receiving such services; or
    - imposing conditions or limitations on the ability of the CTP to provide services to firms and FMIs, and/or firms and FMIs receiving these services.

7.5 Some of the supervisory authorities' powers may only be exercised where the supervisory authority considers that the CTP has contravened a requirement imposed on them. So before these powers could be used, there would need to be an investigation to establish whether the CTP had breached an applicable requirement. To enable these investigations, and ensure that CTPs benefit from due process prior to the exercise of available powers, the FSM Bill proposes to give the supervisory authorities investigatory powers. As is the case with the supervisory authorities' equivalent statutory powers over firms and FMIs, CTPs would have the right to make representations and appeal to the Upper Tribunal.

7.6 The supervisory authorities would have a duty to exercise their proposed supervisory and enforcement powers (see Chapter 9) over CTPs in a coordinated manner. In addition, the FSM Bill proposes to require the supervisory authorities to issue a statement of policy (SoP) setting out how they would exercise their statutory powers over CTPs. The supervisory authorities would envisage consulting on this SoP after the FSM Bill receives Royal Assent. The supervisory authorities would also take into account any inadvertent risk of disruption to the non-UK operations of internationally active firms and FMIs that could result from the exercise of their proposed powers.

7.7 In order to facilitate the proportionate and targeted use of the supervisory authorities'

proposed disqualification powers, the FSM Bill would enable them to exercise it in respect of either:

- all the services that a CTP provides to all relevant firms and FMIs;
- all the services that a CTP provides to some firms or FMIs;
- some of the services that a CTP provides to all relevant firms and FMIs; or
- some of the services that a CTP provides to some firms or FMIs.

7.8 The proportionate and targeted exercise of these powers where appropriate could help mitigate the systemic risks to the supervisory authorities' objectives posed by CTPs. For instance, the Bank has previously used its powers of direction under [Section 191 of the Banking Act 2009](#) <sup>↗</sup> to require FMIs to carry out specific remediation actions. The use of this power followed operational incidents that were similar in nature and potential impact to those that could arise at CTPs.

7.9 Chapter 6 of this DP considered the potential use of the supervisory authorities' proposed statutory power to require skilled persons' reviews of CTPs as one of several potential forms of resilience testing. The supervisory authorities could also use these proposed powers to appoint skilled persons to:

- assess CTPs' implementation of actions required by the supervisory authorities; and
- report their findings to the supervisory authorities. The use of skilled persons in this context could be a proportionate and resource-efficient application of the supervisory authorities' proposed statutory powers.

## 8: International coordination and engagement

---

8.1 This chapter summarises recent and ongoing discussions relating to CTPs at international standard-setting bodies (SSBs), the G7 and other relevant jurisdictions such as the EU. It also discusses potential ways to strengthen global regulatory and supervisory coordination in order to manage the potential systemic risks posed by CTPs.

8.2 Some potential CTPs provide services to firms and FMIs in multiple jurisdictions. Therefore, the potential systemic risks that their failure or severe disruption to their services could pose would not be confined to the UK.

8.3 In addition, as noted by the FPC in Q2 2021 FPS and Record, there are limits to the extent to which financial regulators in any given jurisdiction can, by themselves, mitigate the risks posed by certain CTPs, such as CSPs due to the fact that they provide their services in multiple jurisdictions.

8.4 Internationally active firms and FMIs have also noted that fragmented regulatory and supervisory practices can be detrimental to their operational resilience and increase compliance costs.

**8.5 The supervisory authorities are only able to introduce measures to advance their objectives. Therefore, the potential measures set out in this DP would be limited to the provision of services by CTPs to UK firms and FMIs as defined in Chapter 1. However, the supervisory authorities are mindful of the challenges posed by regulatory and supervisory fragmentation, and the corresponding need for ongoing international regulatory and supervisory alignment.**

## International initiatives relevant to CTPs

### Financial Stability Board (FSB)

8.6 In recent years, the FSB has led global discussions on regulatory and supervisory issues relating to firms and FMIs' outsourcing and third party relationships, including the potential systemic risks posed by CTPs.

8.7 A DP published by the FSB in November 2020 on '[Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships](#)' (FSB DP) identified a common concern about "the possibility of systemic risk arising from concentration in the provision of some outsourced and third party services to [financial institutions (FIs)]." The FSB DP noted that "where there is no appropriate mitigant in place, a major disruption, outage or failure at one of these third parties could create a single point of failure with potential adverse consequences for financial stability and/or the safety and soundness of multiple financial institutions." The FSB DP also examined:

- the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third party relationships (including risks in sub-contractors and the broader supply chain);
- possible ways to address these challenges and mitigate related risks, including in a cross-border context; and
- lessons learnt from Covid-19 relating to outsourcing and third party relationships.

8.8 The FSB DP received 39 responses, which (among other points) noted that:

- "concentration of critical services in the same third-party service provider by financial institutions may create risks to the financial system"; and
- "identifying, monitoring and managing systemic concentration risk in the provision of third-party services and other interdependencies is beyond the responsibility of individual financial

institutions.”

8.9 Following the industry response to its DP, the FSB is undertaking further work in this area, which will focus on the development of:

- common definitions and terminologies on outsourcing and third party risk management; and
- expectations for financial authorities’ oversight of financial institutions’ reliance on service providers that authorities or financial institutions deem critical.

## **Basel Committee on Banking Supervision (BCBS)**

8.10 In March 2021, the BCBS published a set of [Principles for Operational Resilience](#) (POR). The POR align to the supervisory authorities’ operational resilience framework. While the POR do not explicitly address the potential systemic risks posed by CTPs, several principles are relevant to them, such as Principle 5, which deals with third party dependency management.

8.11 In late 2021, the BCBS held outreach sessions with private sector participants and supervisory authorities from various jurisdictions to assess the status of more well-established practices related to third party risk management, and to exchange views regarding evolving practices related to fourth-party risk management and concentration risk matters. The topic of potential systemic risk stemming from concentration in the provision of third party services to banks featured in these sessions.

8.12 The Bank for International Settlements (BIS) has also established an ‘Innovation Hub’ and a ‘Cyber Resilience Coordination Centre’, which could help improve cross-border regulatory and supervisory coordination in these areas (see [BIS Annual Report 2020/21](#) pages 81-91).

## **CPMI-IOSCO**

8.13 In October 2021, IOSCO issued revised ‘[Principles on Outsourcing](#)’, which apply to market intermediaries, trading venues, market participants acting on proprietary basis, and credit rating agencies (collectively ‘regulated entities’). FMIs may also consider their application.

8.14 The revised IOSCO framework comprises a set of fundamental precepts and seven principles. Principle 5 covers concentration risk from the perspective of individual regulated entities. However, it noted that ‘where multiple regulated entities use a common service provider, operational risks are correspondingly concentrated, and may pose a threat of systemic risk’.

8.15 The CPMI-IOSCO Working Group on Cyber Resilience (WGCR) is currently focusing on strengthening the cyber resilience of FMIs in line with the 2016 [CPMI-IOSCO Guidance on Cyber Resilience for FMIs](#). As part of this process the WGCR is currently undertaking a review of the Cyber Guidance to assess whether it needs to be updated, augmented, or changed. In January 2022 IOSCO issued [consultation report](#) on Operational resilience of trading



venues and market intermediaries during the Covid-19 outbreak. The discussion paper examines the operational resilience of regulated entities during the outbreak. In particular, the paper examines the key operational risks and challenges that regulated entities faced during the pandemic such as the rapid and widespread shift to remote working, the subsequent rise of hybrid working in many jurisdictions, and increased reliance on IT systems and third parties. The paper also highlights that outbreak also increased cyber security risks, accelerated the adoption and use of existing, new and emerging technologies and created disruptions to arrangements with third parties.

### **G7 Cyber Experts Group (CEG)**

8.16 The G7 CEG has issued several Fundamental Elements relating to the cyber resilience of the global financial services sector. Some of these Fundamental Elements could help facilitate cross-border resilience testing of CTPs (see Testing section below for details).

### **International Association of Insurance Supervisors (IAIS)**

8.17. The IAIS Operational Resilience Task Force (ORTF) is currently working on development of an Issues Paper that focuses on operational resilience in the insurance sector, specifically on IT third party outsourcing and insurance sector cyber resilience.

### **Regional and national initiatives**

8.18 In addition to the global initiatives highlighted above, there are a number of ongoing national and regional initiatives relevant to CTPs, including the EU's Digital Operational Resilience Act (DORA), which Box E summarises.

#### **Box E: The EU's Digital Operational Resilience Act (DORA)**

In September 2020, the European Commission (EC) published a legislative proposal for a Regulation on digital operational resilience for the financial sector (known as 'DORA') as part the EU's Digital Finance package. DORA aims to harmonise the regulation and supervision of digital operational resilience and ICT risk management across the EU finance sector.

DORA will apply to 20 types of EU 'financial entity', including banks, CCPs, CSDs, insurers and investment firms. It covers six main areas: scope and proportionality; definitions; ICT governance and risk management; ICT incident reporting; digital operational resilience testing, and ICT third party risk management.

The section on ICT third party risk management in DORA includes provisions for the creation of an EU oversight framework for critical ICT third party service providers to EU

financial entities, including CSPs.

Under this oversight framework, the European Supervisory Authorities (ESAs) will designate critical ICT third party service providers based on criteria such as their substitutability and the potential systemic impact they could cause if they experienced a large operational failure. The ESAs will update and publish an annual list of critical ICT third party service providers and appoint either the EBA, EIOPA and/or ESMA as ‘Lead Overseer’ of critical ICT third party service providers. Critical ICT third party service providers will also be required to maintain an establishment in the EU, ie a subsidiary, to provide their services.

Lead Overseers will perform an annual, tailored assessment of each critical ICT third party service provider assigned to them. They will have powers to request relevant documents and information, conduct inspections and issue recommendations to critical ICT third party service providers (ie using a specific cybersecurity tool, or not sub-contracting critical or important functions to ‘nth parties’ outside the EU).

Lead Overseers will also have the power to fine critical ICT third party service providers who failed to comply with requests for access, documents or information. National Competent Authorities will likewise have powers to suspend or terminate the provision of services by ICT critical third party service providers to financial entities in their jurisdictions in certain circumstances.

At the time of publication of this DP, the EU legislative bodies had announced that they had reached a provisional compromise on DORA. Once it is adopted, the ESAs will be required to issue a range of joint Implementing Technical Standards, Regulatory Technical Standards (RTSs) and Guidelines.

## Potential ways to improve international coordination on CTPs

8.19 Given the number of international and regional initiatives relevant to the potential systemic risks posed by CTPs, global regulatory and supervisory coordination among financial supervisory authorities will continue to be important in the future. The rest of this chapter discusses potential ways to strengthen international coordination.

### A global methodology for identifying CTPs

8.20 While a global framework for designating CTPs could be challenging to agree and operate in practice, a global methodology for identifying potential CTPs, including high-level criteria, could be more attainable highly desirable. Similar methodologies aimed at designating globally systemically significant financial institutions (G-SIFIs) already exist. For instance:

- [SCO40 of the Basel Framework](#), which is used in the designation of globally systemically important banks;
- the [IAIS Updated Assessment Methodology for globally systemically important insurers](#); and
- the [FSB's Assessment Methodologies for Identifying Non-Bank Non-Insurer Global Systemically Important Financial Institutions - Proposed High-Level Framework](#).

8.21 The methodologies referred to above use similar high-level criteria to the potential criteria for identifying CTPs in the FSM Bill and examined in detail in Chapter 4 of this DP (eg market share, complexity, concentration, interconnectedness, substitutability etc.), albeit tailored to the characteristics of different types of G-SIFI. A set of high-level criteria to identify 'global' CTPs could improve consistency and cooperation among financial supervisory authorities.

8.22 A potential obstacle to the development of a common methodology for identifying global CTPs could be inconsistent or insufficient data on firms' and FMIs' third party dependencies across jurisdictions. Therefore, greater standardisation on the information that financial supervisory authorities around the world collect about these dependencies could be very valuable. The BCBS's [Principles for effective risk data aggregation and risk reporting](#) and wider work on legal entity identifiers could provide useful lessons for potential, future relevant initiatives.

### Global resilience standards for CTPs

8.23 As discussed in Chapter 5, there are already global standards directly applicable to critical service providers to FMIs, such as Annex F of the CPMI-IOSCO Principles for FMIs and the High Level Expectations for the Oversight of SWIFT.

8.24 The supervisory authorities consider that a global set of principles-based, minimum resilience standards aimed at CTPs to the finance sector as a whole could be an important and valuable tool for managing the potential, cross-border systemic risks that they may pose. Such standards could promote a common, global, minimum level of resilience for CTPs. They could also help reduce regulatory fragmentation and mitigate compliance costs for internationally active firms and FMIs. Potential global standards for CTPs could cover similar areas to those covered by the potential standards for CTPs discussed in Chapter 5 of this DP. A particularly helpful area for potential global standards to cover could be the response and recovery capabilities of CTPs in case of failure or disruption to their services.

### Cross-border resilience testing of CTPs

8.25 There are several precedents of cross-border collaboration among financial supervisory authorities involving sector-wide exercises and cyber-resilience testing of firms and FMIs. Bringing CTPs into future cross-border sector-wide exercises and, if appropriate, cyber-

resilience tests could help strengthen the resilience of the global financial system.

### **Sector-wide exercises**

8.26 In June 2019, the G7 CEG delivered the first cross-border coordination exercise across the G7 (involving 23 financial supervisory authorities). Following this exercise, the G7 CEG agreed to make simulation exercises a permanent part of its mandate and developed the '[G7 Fundamental Elements of Cyber Exercise Programmes](#)'<sup>27</sup> as a framework for future exercises. The BIS's CRCG mentioned above has also hosted and taken part in sector-wide exercises.

8.27 The G7 Fundamental Elements of Cyber Exercise Programmes are addressed to 'financial institutions' but recognise the potential role of other stakeholders in these exercises. For instance, the planners of these exercises should "assess their interconnections to other companies and the companies upon which they are operationally dependent, eg, third party service providers, often referred to as an ecosystem scan." Planners may also 'consider including such experts from departments representing communications, legal, business line owners, sister agencies, law enforcement, and critical third parties such as internet service providers or telecommunications in exercises.

### **Cyber resilience testing**

8.28 In 2018, the G7 published the [Fundamental Elements for Threat Led Penetration Testing Data](#)<sup>28</sup> (TLPT) to 'provide core elements of and approaches for the conduct of TLPT across G-7 jurisdictions' and "facilitate greater compatibility among TLPT approaches."

8.29 Like the G7 Fundamental Elements of Cyber Exercise Programmes, the Fundamental Elements for TPLT are addressed to financial institutions but note that they "should identify the underlying people, processes and technology supporting those critical functions and services, including third party providers (such as IT service providers and supply chain relationships). If the test requires the inclusion of third party providers within the scope, it is the responsibility of the entity to liaise and ensure the participation of the third party provider."

8.30 The supervisory authorities have previously worked with the European Central Bank (ECB) and other EU Authorities to conduct CBEST testing on a cross-jurisdictional basis and align with similar frameworks such as TIBER-EU.

8.31 Article 23 of the DORA compromise text provides for the possibility of ICT third party service providers contractually agreeing with firms and FMIs that they could enter into arrangements with external testers "on behalf of all their financial entity service users in order to conduct pooled [TPLT] testing." This testing could provide an alternative method to conduct or facilitate cross-border cyber-resilience testing of CTPs.

8.32 The supervisory authorities are interested in suggestions for additional ways to improve international coordination with overseas supervisory authorities in order to manage any cross-border systemic risks that CTPs may pose.

### **Recognition of tests undertaken by non-UK financial supervisory authorities**

8.33 The supervisory authorities could also take into account resilience tests, sector-wide exercises and other oversight activities undertaken by or on behalf of non-UK financial supervisory authorities on CTPs. However, this could be without prejudice to their ability to carry out additional testing if appropriate. It could also depend on factors such as the:

- extent of the supervisory authorities' awareness of, and involvement in these resilience tests, sector-wide exercises and oversight activities; and
- level of assurance that these resilience tests and exercises provided about the resilience of any material services that CTPs provide to firms and FMIs specifically.

### **Questions**

1. Could a set of global, minimum resilience standards for CTPs be helpful? If so, what areas should these standards cover?
2. What additional steps could financial supervisory authorities around the world take to enable resilience testing of CTPs to be coordinated effectively on a cross-border basis?
3. What forms of testing could be most appropriate (ie sector-wide exercises, TPLT or other forms)? Are there any practical challenges in these cross-border exercises which the supervisory authorities should anticipate and manage?
4. Are there any other ways not covered in this DP to improve international regulatory and supervisory coordination in relation to the risks posed by CTPs?
5. What are your views on the possibility of the supervisory authorities taking into account resilience tests, sector-wide exercises and other oversight activities undertaken by or on behalf of non-UK financial supervisory authorities on CTPs (subject to certain conditions)?

## **9: Coordination with UK competent authorities and public bodies outside the finance sector**

---

9.1 Some potential CTPs may also provide services to organisations outside the finance sector, including some that are part of the UK's critical national infrastructure. The powers envisaged under the FSM Bill, and the potential measures set out in this DP, are not designed to cover these wider services. The supervisory authorities would have powers only over CTPs' provision of

services to firms and FMIs, and would have no role in overseeing or supervising CTPs as legal entities in their own right, or their provision of services outside the financial sector.

9.2 There are cross-sectoral legislative frameworks relevant to the services that some CTPs provide. However, they do not eliminate the need for the finance sector-specific measures discussed in this DP due to the fact that they:

- do not specifically address the supervisory authorities' objectives, including their shared objective of financial stability;
- may not cover all potential CTPs; and
- may have varying levels of regulatory and supervisory maturity.

9.3 Nevertheless, the supervisory authorities consider it important to coordinate with relevant UK competent authorities and public bodies outside the finance sector with a potential interest in certain CTPs. The rest of this chapter identifies areas where coordination with these competent authorities and bodies could be developed.

9.4 The FCA already has a [MoU with the Information Commissioner's Office \(ICO\)](#). However, enhanced cooperation is likely to require new or amended formal arrangements between the supervisory authorities and relevant UK competent authorities and public bodies outside the finance sector, which may include but not necessarily be limited to:

- the National Cyber Security Centre (NCSC), which already engages with the supervisory authorities and HMT (including via the ARF);
- members of the Digital Regulation Cooperation Forum (DRCF). In particular, the Information ICO as the UK competent authority responsible for supervision of:
  - data protection under the Data Protection Act 2018; and
  - digital service providers (DSPs) under the Network and Information Systems Regulations (NISR), summarised in Box F below.

### **Box F: The Network and Information Security Regulations (NISR)**

The Network and Information Systems (NIS) Directive sought to improve cybersecurity in the EU by requiring Member States to:

- identify
  - operators of essential services (OESs), and
  - digital service providers (DSPs) in their jurisdictions; and
- apply minimum cyber security and incident reporting requirements to OESs and DSPs.

NISR, which came into force in May 2018, transposed the NIS Directive into UK law.

OESs are entities that provide essential services for the maintenance of critical societal and/or economic activities. Although some firms and FMIs could meet the definition of an OES, the finance sector is outside the scope of NISR due to the fact that, at the time of implementation, it was 'deemed to have had equivalent or better regulation already in effect'.

The most relevant part of NISR as far as CTPs are concerned is the regime for DSPs, which currently includes CSPs, online marketplaces and search engines. NISR requires DSPs to:

- register with the ICO;
- implement appropriate and proportionate IT security measures;
- prevent and minimise the impact of incidents on the continuity of their services; and
- notify the ICO within 72 hours of becoming aware of any incident having a 'substantial impact' on the provision of their services.

The ICO supervises DSPs and has powers of inspection and enforcement over them. However, at present, it only subjects them to light-touch and reactive ex post supervisory activities.

In January 2022, the Department for Digital, Culture, Media and Sport (DCMS) published a consultation on '[Proposals for legislation to improve the UK's cyber resilience](#)', which would amend various parts of NISR, including the supervisory regime for DSPs. The proposed amendments would:

- expand the scope of the DSPs regime to 'managed service providers' (MSPs) ie providers of managed IT services, such as
  - security,
  - business process outsourcing;
  - analytics/artificial intelligence; and
  - business continuity and disaster recovery; and
- introduce a two-tier supervisory regime for DSPs:
  - a proactive regime for the most critical DSPs, and
  - a reactive regime for all others.

The proposed, revised supervisory regime for DSPs, including the criteria to identify those that are critical, would be left to the ICO. DCMS's consultation explicitly noted that 'there may be opportunities for cross-sectoral collaboration with sectoral initiatives either within

or outside of the NIS framework when it comes to establishing thresholds for inclusion or identifying the most critical digital services, for example in the financial services sector, where digital services play a critical role’.

DCMS’s consultation also proposes expanding its incident reporting requirements for OESs to incidents that do not actually affect the continuity of the service directly, but nonetheless pose a significant risk to the security and resilience of the entities in question and the essential services they provide (eg ransomware attacks). These possible approaches outlined in this DP could also create opportunities for collaboration between the supervisory authorities and the ICO.

DCMS’s consultation also proposes a new power for HM Government to designate critical suppliers of services to OESs in the various sectors covered by NIS (eg healthcare, transport etc.) thus bringing them into the NIS framework. The proposals in this DP could potentially support similar initiatives to monitor and strengthen resilience of critical suppliers to sectors covered by the NIS framework.

## Designation of CTPs

9.5 As noted in Chapter 4, the supervisory authorities expect to engage with relevant UK competent authorities and public bodies outside the finance sector before recommending to HMT that it designates a third party as a CTP. HMT would also have a statutory duty to notify relevant authorities before designating a third party as a CTP.

9.6 As noted in Chapter 4, the supervisory authorities would ultimately decide which third parties to recommend for designation as CTPs to HMT based on their assessment of the potential systemic risks to their objectives. However, certain competent authorities and public bodies outside the finance sector may have relevant information to contribute to the supervisory authorities’ assessment.

9.7 Moreover, some of the potential criteria that DCMS and the ICO are considering to identify ‘critical’ DSPs under the proposed revisions to NISR are consistent with those discussed in Chapter 4, which opens up further opportunities for regulatory and supervisory coordination between the supervisory authorities and the ICO.<sup>[12]</sup>

## Resilience Standards

9.8 As noted in Chapter 5, the supervisory authorities would take into account compliance with recognised certifications and standards as partial or supporting evidence that CTPs met their possible minimum resilience standards for CTPs. These certifications and standards include those issued by relevant UK competent authorities and public bodies, such as the [NCSC’s](#)



[Cyber Essentials Plus](#) and [Cloud Security Principles](#), as well as any standards for DSPs that the ICO may introduce in the future.

## Testing

9.9 Joint, cross-sectoral resilience testing of CTPs could, in theory, be possible. Regulation 16(2) of NISR empowers the ICO to conduct an inspection; appoint a person to conduct an inspection on its behalf; or direct that a DSP appoint a person who is approved by the ICO to conduct an inspection on its behalf. Subject to further legal analysis and appropriate cooperation arrangements, the supervisory authorities could explore the possibility of carrying out some of the possible resilience tests in Chapter 6 jointly with the ICO on any CTPs that might also be classed as DSPs under the NIS Regulations.

## Incident reporting

9.10 As mentioned in Chapter 5, the possible resilience standards for CTPs would, if introduced, require them to promptly and proactively provide information ‘relating to incidents or threats capable of having a systemic impact on their objectives’. The supervisory authorities also plan to consult on operational incident reporting requirements for firms and FMIs in 2023.

9.11 Regulation 12 of NISR already requires DSPs to notify the ICO of incidents “having a substantial impact” on the provision of any relevant digital services not later than 72 hours after becoming aware of them. DCMS is proposing to expand the incident reporting requirements in NISR to “security incidents that have an impact on the security of network and information systems underpinning the provision of an essential service but do not affect the continuity of that service.”

9.12 Likewise [Section 67 of the Data Protection Act 2018](#) requires controllers of personal data to notify data breaches of personal data for which they are responsible to the ICO on the same timeframe.<sup>[13]</sup>

9.13 Although there may be differences between, on the one hand, the information that data controllers and DSPs have to report to the ICO following an incident, and the information that firms and FMIs and CTPs may be required to report to the supervisory authorities in future, there could be efficiencies and other benefits in establishing formal mechanisms for sharing information on incidents of mutual interest between the supervisory authorities and the ICO.

## Questions

1. Are there any other areas besides those discussed in this DP where cross-sectoral cooperation could be developed to support the possible measures for CTPs discussed in this DP?

## 10: Questions

---

1. Do you agree with the supervisory authorities' overview of the potential implications of firms' and FMIs' increasing reliance on third parties (in particular the potential systemic risks to the supervisory authorities' objectives)? Is there anything else that the supervisory authorities should consider in their analysis?
2. Do you agree with the supervisory authorities' assessment of the limitations of the current regulatory framework?
3. Do you agree that, when considering potential requirements for CTPs, it is appropriate for the supervisory authorities to focus on (a) minimum resilience standards, and (b) resilience testing, in respect of the material services that CTPs provide to firms and FMIs? Are there any alternative or additional areas that the supervisory authorities should consider?
4. Do you agree with the potential advantages in aligning the potential measures for CTPs to the existing operational resilience framework for firms and FMIs? Are there additional ways in which the potential approach to CTPs could be aligned to the existing operational resilience framework? Are there alternative approaches the supervisory authorities should consider?
5. What are your views on the factors that the supervisory authorities should consider when assessing which third parties to recommend for designation as CTPs? Are there any aspects of the criteria discussed above that the supervisory authorities should clarify, develop or omit? Are there any additional factors that the supervisory authorities should take into account?
6. What are your views on the supervisory authorities' potential approach for assessing concentration, materiality and potential impact in the provision of third party services to firms and FMIs? Are there alternative approaches for doing so that could be more effective or pragmatic?
7. What are your views on how best to take into account potential linkages with other regimes outside financial services when considering the recommendation of third parties as CTPs to HMT? How could the supervisory authorities improve coordination with other competent authorities and public bodies outside the finance sector?
8. What are your views on how best to avoid or mitigate potential unintended consequences, including potential distortion, such as deterring third parties from entering the market or providing services to firms and FMIs, as a result of a third party being designated as a CTP?
9. Are the supervisory authorities' potential resilience standards for CTPs clear, comprehensive and proportionate? Are there any standards that the supervisory authorities could add, clarify, omit or review?
10. What relationship, if any, should recognised relevant certification and standards have with the supervisory authorities' possible minimum resilience standards for CTPs?
11. What are your views on the potential costs and benefits of complying with the minimum

resilience standards discussed in this DP?

12. What are your views on the potential resilience testing tools for CTPs discussed in this chapter? Are there any additional or alternative tools that the supervisory authorities could consider applying to CTPs?
13. How could the supervisory authorities work with CTPs, firms and FMIs and other stakeholders to make resilience testing of CTPs efficient, proportionate and resource-effective?
14. In terms of the different potential forms of cyber-resilience testing discussed in this chapter, are there any that could be particularly effective for CTPs? Conversely, are there any that could be particularly difficult to implement in practice or give rise to unintended consequences?
15. What do you think could be the most effective way for the supervisory authorities to share the findings and recommended actions of any resilience testing performed by or on CTPs with, at least, those firms and FMIs that rely on them for material services? How could the supervisory authorities balance the need to share this information with relevant firms and FMIs with potential confidentiality or market sensitivity considerations? Could a rating system along the lines of the URSIT system used by the FFIEC in the US promote clarity and consistency in supervisory authorities' assessments?
16. Could a set of global, minimum resilience standards for CTPs be helpful? If so, what areas should these standards cover?
17. What additional steps could financial supervisory authorities around the world take to enable resilience testing of CTPs to be coordinated effectively on a cross-border basis?
18. What forms of testing could be most appropriate (ie sector-wide exercises, TPLT or other forms)? Are there any practical challenges in these cross-border exercises which the supervisory authorities should anticipate and manage?
19. Are there any other ways not covered in this DP to improve international regulatory and supervisory coordination in relation to the risks posed by CTPs?
20. What are your views on the possibility of the supervisory authorities taking into account resilience tests, sector-wide exercises and other oversight activities undertaken by or on behalf of non-UK financial supervisory authorities on CTPs (subject to certain conditions)?
21. Are there any other areas besides those discussed in this DP where cross-sectoral cooperation could be developed to support the possible measures for CTPs discussed in this DP?

## **Annex 1: Academic, industry and international publications on CTPs**

---

In recent years, multiple publications by academia, industry, UK public bodies, and international organisations have highlighted the growing systemic risks posed by certain third parties to the

financial services sector. Some of these publications, which helped inspire some of the potential measures examined in the main body of the DP, are summarised below.

## Publications by UK public bodies

The [National Cyber Security Centre's \(NCSC\) Annual Review](#) <sup>↗</sup> monitors the evolving cyber threat landscape. The 2021 Annual Review underscored that disruption at third parties and to their supply chains also appears to be an increasing risk. It highlighted that there were a rising number of cyber incidents in 2021, which highlighted the “viability, effectiveness and global reach of supply chain operations as a means of compromising comparatively well-defended targets.” The 2021 Review also warned that “further such operations are almost certain over the next twelve months.”

During 2022, the NCSC also highlighted the heightened risk of cyber threats due to geopolitical issues, and published targeted [guidance](#) <sup>↗</sup>, including on supply chain risk management. This guidance reflects the core aim of limiting the UK’s “reliance on individual suppliers or technologies which are developed under regimes that do not share our values,” which was highlighted in the foreword to the UK Government’s [National Cyber Strategy 2022](#) <sup>↗</sup>.

## Publications by international bodies

Concerns about the potential financial stability risks posed by certain third parties are not limited to the UK highlighting the importance of cross-border cooperation in this area. Chapter 8 of the DP already covered the Financial Stability Board’s November 2020 Discussion Paper on [‘Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships](#) <sup>↗</sup>.

In addition, a report on [‘Systemic Cyber Risk’](#) <sup>↗</sup> by the ESRB (ESRB Report I) published in February 2020 concluded that:

- a cyber-incident, including a failure or outage at a third party, could give rise to systemic cyber risk if it led to an erosion of trust in the financial system. Such an erosion of trust would necessitate a level of disruption to critical functions supporting the real economy, or a level of generated (or anticipated) financial losses that the financial system could not absorb; and
- insufficient oversight of third party providers and supply chains was both the most common, and the highest priority vulnerability that could lead to systemic cyber risk.

A follow-up report on [‘Mitigating Systemic Cyber Risk](#) <sup>↗</sup> published by the ESRB in January 2022 (ESRB Report II) proposed a range of measures for mitigating potentially systemic cyber risks. In particular, it noted that:

- the identification of systemic nodes, including certain ICT third party providers is of the utmost

importance for the monitoring and analysis of systemic cyber risk; [14] and

- these systemic nodes should operate with elevated levels of cyber resilience. To achieve this, the report recommended their inclusion in systemic cyber resilience scenario stress testing.

A paper on **[‘BigTech in Financial Services’: Regulatory Approaches and Architecture](#)** published by the IMF in 2022, concluded that the importance of services such as cloud to the finance sector “means that, in some respects, BigTechs are already too big to fail.”

These publications highlighted the systemic risks to the supervisory authorities’ objectives posed by CTPs, and informed some of the potential measures discussed in this DP. For instance, a paper on **[‘Systemic consequences of outsourcing to the cloud’](#)** published by the London School of Economics in December 2019, concluded that:

- the cloud is a critical infrastructure that is controlled by a handful of companies whose failure would be catastrophic; and
- cloud vendors are systemically important and should be designated and regulated accordingly.

A paper by the Financial Stability Institute (FSI) of the Bank for International Settlements on **[‘Big tech interdependencies – a key policy blind spot’](#)** published in July 2022, also examined some of the systemic risks posed by CTPs as part of a wider analysis of the “increasingly prominent role of large technology firms (big techs) in the financial sector” and the questions it raises regulation. The FSI paper looked at various ways in which BigTechs interact with the financial services, including as direct providers of selected financial services eg credit provision and payments; as strategic partners with regulated financial institutions, and as CTPs.

The FSI paper noted that the “growing reliance by a large number of financial institutions on technology services provided by a small number of big techs makes the continuity of those services systemically relevant. This dependency is forming single points of failure, and hence creating new forms of concentration risk, which “is particularly evident in the cloud services market”. “Because there are no readily available substitutes or infrastructures for these services”, the paper argues, “a disruption in one of these big techs could have systemic implications for the financial system. Therefore, the need for big techs to implement best-in-class operational resilience and cyber security frameworks is an imperative to mitigate financial stability risks.”

The FSI paper ultimately recommended the “development of specific entity-based rules for big tech operations in the financial sector”, which should capture not just the provision of a services to financial institutions, but “the combination of all financial and non-financial activities they perform”. The paper also noted the move towards direct regulatory oversight over providers of critical services in certain jurisdictions, and recommended that authorities ramp up their monitoring efforts of regulated entities’ use of critical services to identify risks “including concentration and contagion risks and, at the macro level, systemic risks”. The paper notes that this could be “undertaken through – or in concert with – industry-wide business continuity plan (BCP) testing”

along the lines discussed in Chapters 5 and 6 of this DP.

## Industry publications

Industry publications have been tracking the financial sector's growing reliance on cloud service providers (CSPs).

For instance, a study by McKinsey referenced in the Bank's '[Future of Finance Report](#)', which was published in June 2019, predicted that 40%-90% of banks' workloads globally could be hosted on the cloud within a decade (a workload in this context is an application, service, capability or a specific amount of work that can be run on the cloud). The report also found that the top four CSPs had a combined market share of 65% among UK firms.

Two surveys by Ernst and Young (EY) published in November 2020 ([UK Banking public cloud adoption: banks must think big to transform](#)) and February 2021 ([How insurers can transform by adopting public cloud](#)) respectively found that 27% of banks and 49% of insurers plan to move the majority of their business to the cloud in the next few years.

Many industry publications coincide that the Covid-19 outbreak accelerated the implementation of many firms' and FMIs' digital transformation plans. A [survey](#) by UK Finance, Google, and EY published in November 2021 showed that nearly a third of UK Finance members agreed that cloud adoption had accelerated during the outbreak.





The Carnegie Endowment for International Peace has published a number of papers relevant to the issues discussed in this DP as part of a project on 'Cybersecurity and the financial system'. These publications include a paper on '[Systemic Cyber Risk: A Primer](#)', published in March 2022. The paper identifies risk concentration, complexity and opacity and scale (all of which are features of CTPs) as potential causes of systemic cyber risk. The paper also considers potential tools that policymakers could use to manage systemic cyber risk, including some that are relevant to the potential measures in this DP, eg:

- developing a framework for identifying "systemically important digital entities—those most at risk of triggering, propagating, or suffering the effects of systemic cyber events" inspired by existing frameworks for the identification of systemically important financial institutions;
- convening international, multi-stakeholder working groups, perhaps under the aegis of existing industry or international forums or trusted nongovernmental organizations, to focus on different sources of concentrated risk.

## Academic publications

A paper on '[Systemic consequences of outsourcing to the cloud](#)' published by the London School of Economics in December 2019, concluded that:

- the cloud is a critical infrastructure that is controlled by a handful of companies whose failure would be catastrophic; and
  - cloud vendors are systemically important and should be designated and regulated accordingly.
- 

1. The FSM Bill uses two terms to refer to 'firms' as defined in this DP. The term 'authorised persons', which is used throughout FSMA. The Bill also uses the term 'relevant service providers' as an umbrella term for two types of 'firm' namely payment and e-money institutions.
2. The FSM Bill refers to FMIs as 'FMI entities', and to CCPs as 'recognised clearing houses'.
3. Although the definition of an 'availability zone' varies slightly among different CSPs, it generally comprises physically separate data centres in a single geographic region with redundant connectivity, networking and power. These features can enhance a CSP's tolerance to local disruption.
4. This DP uses the same definition of a 'single-point-of-failure' as the [CPMI-IOSCO Principles for FMIs](#)  ie "any point in a system, whether a service, activity, or process, that, if it fails to work correctly, leads to the failure of the entire system."
5. Certain firms and FMIs have to carry out similar, regular self-assessments and submit them to the supervisory authorities. For instance, specified service providers to payment systems are **expected** to complete a self-assessment against the expectations in Annex F of the CPMI-IOSCO Principles for FMIs every two years, and to provide this to the Bank. In the alternate years, specified service providers should complete and submit a top down strategic review. Likewise, Payment Service Providers, are **required**  to perform regular self-assessments against the 'EBA's Guidelines on security measures for operational and security risks of payment services' (EBA/GL/2017/17).
6. The proposed designation criteria for CTPs in the FSM Bill was also informed by international thinking about the risks that CTPs may pose to financial stability. For instance, see Element 5 of the '[G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector](#)' .
7. From 1 January 2023, the definition of 'critical services' in the PRA Rulebook will also include services necessary to deliver a firm's core business lines.
8. As Chapter 1 notes, the proposed definition of 'third party' in the FSM Bill would include persons connected to a third party, such as nth parties.
9. The CAF is intended for use 'by organisations that are responsible for services and activities that are of vital importance to us all'. For instance, organisations within the UK Critical National Infrastructure (CNI); organisations subject to NIS Directive cyber regulation (see Chapter 9); and organisations managing cyber-related risks to public safety.
10. The Basel Committee on Banking Supervision (BCBS) **defines**  'step-in' risk as 'the risk that a bank may provide financial support to an entity beyond or in the absence of any contractual obligations, should the entity experience financial stress.'
11. The supervisory authorities published the **high-level findings** of the SIMEX 18 exercise conducted in 2019, which involved a cyber-attack scenario targeting the financial sector.
12. The potential criteria for identifying 'critical' DSPs being considered by DCMS in its 'Proposal for legislation to improve the UK's cyber resilience' include: market reach (ie the number of users relying on the service provided); scale of service provided; financial and/or revenue; concentration in the market; the criticality of the clients supplied; the level of dependence of the clients on the service; the level of connectivity and access to the clients network, and the likely consequences for national security if an incident impacts on the service.

13. Note, however, that some CTPs might be classed as ‘processors’ rather than ‘controllers’ of personal data under the Data Protection Act 2018 and may therefore not be covered by this notification obligation.
14. The ESRB Report II defines ‘systemic nodes’ as agents fulfilling a critical financial or operational role in the financial sector. They are characterised by the importance or a lack of substitutability of the financial or operational services they provide to the financial system.