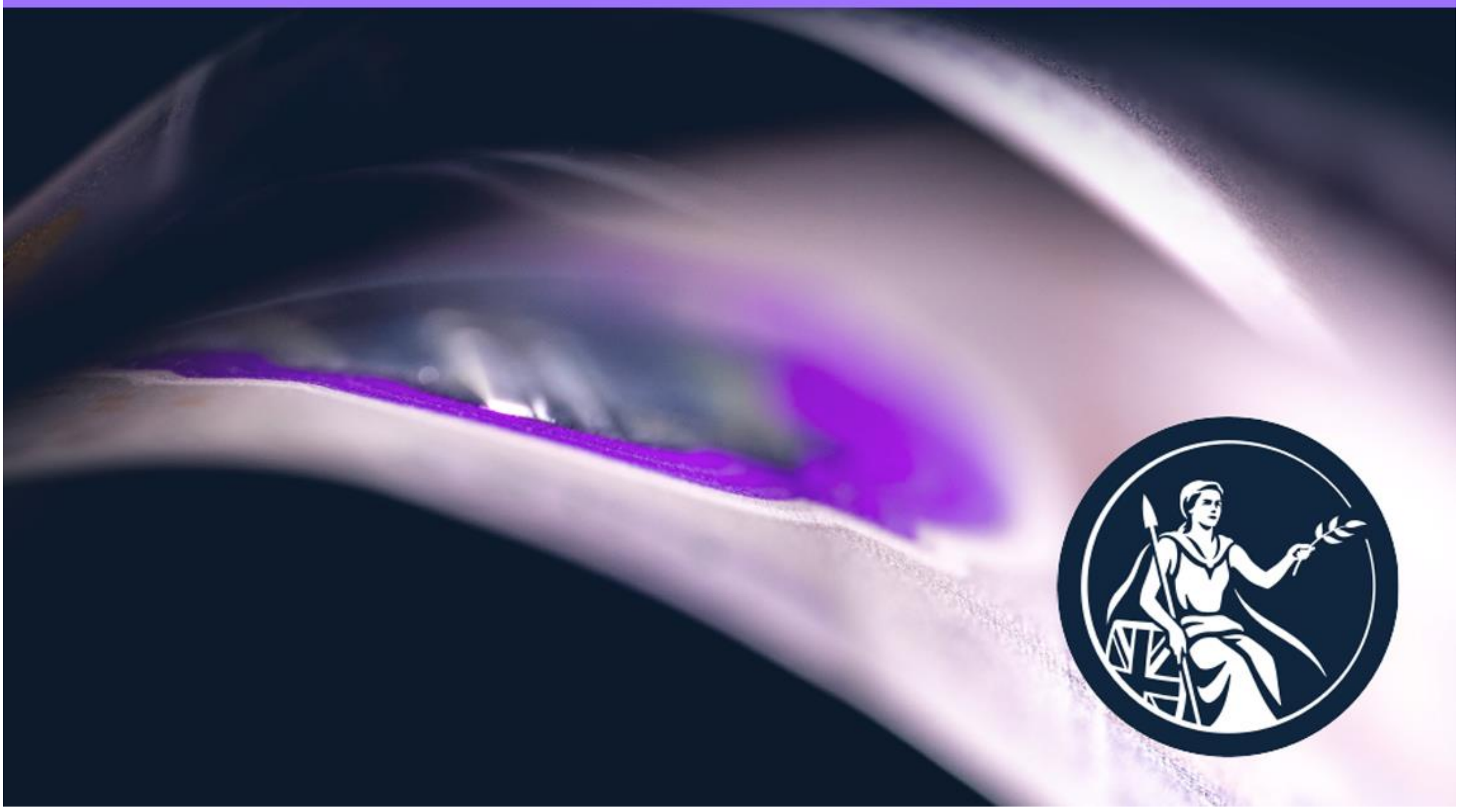
Bank of England PRA

FCA FINANCIAL CONDUCT AUTHORITY

The Regulators' approach to the oversight of critical third parties (The Bank of England, the Prudential Regulation Authority and the Financial Conduct Authority)

November 2024



Contents

Prudential Regulation Authority | 20 Moorgate | London EC2R 6DA

Introduction

We, the Prudential Regulation Authority (PRA), the Bank of England (the Bank), and the Financial Conduct Authority (FCA) (collectively 'the regulators') are the authorities responsible for regulating and overseeing critical third parties (CTPs) to the UK financial sector.

This document acts as a standing reference, setting out how the regulators intend to use the oversight powers granted to us by legislation in respect of CTPs[1], in accordance with and in advancement of our respective statutory objectives.

The regulators aim to promote regulatory accountability and transparency by communicating what CTPs may expect during the course of oversight; in particular recognising that they may not have been previously regulated. The document aims to help the wider market understand the regulators' oversight approach and to aid accountability to the public and Parliament. The document highlights the outcomes-focused and proportionate nature of the regime, not just in the rules and expectations for CTPs, but also in the regulators' approach to oversight.

As this is a new regime, the document may be revised and reissued over time in response to lessons learned and domestic and international developments.

[1] See FSMA 2000, Part 18, Chapter 3C.

1: Background

The CTP regime enables the regulators to directly oversee services that CTPs provide to firms. The regulators will assess CTPs against outcomes-focused rules and expectations, aiming to reduce the risk of systemic disruption by ensuring the services CTPs provide to the financial sector are resilient.

Firms are increasingly dependent on certain third parties for the delivery of functions and services that are essential to the stability of, or confidence in, the UK financial system.[2] In some cases third parties can become so critical that no single firm can adequately monitor or manage the systemic risks a third party poses. These systemic risks may arise when firms rely on a small number of third parties to provide a service or services which, if disrupted, could threaten the stability of, or confidence in, the UK financial system.

After several years monitoring systemic risk from concentration within third parties, 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'.[3] Following this, HM Treasury (HMT) brought forward legislation to enable it to designate certain third parties as 'critical' and giving the regulators the ability to directly oversee the services provided to firms by these critical third parties. The regime has been designed to allow the regulators to intervene in a proportionate manner to raise the resilience of these services and reduce the risk of systemic disruption in the financial sector.

Under this regime, a CTP is an entity that has been designated by HMT in accordance with section 312L of the Financial Services and Markets Act 2000 (as amended) (FSMA). HMT may only designate an entity if, in its opinion, a failure in or disruption to the provision of the services that the third party provides to firms (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK

[2] 'Firms' is an umbrella term for every: i) person authorised by the PRA and/or the FCA, ii) Financial Market Infrastructure, and iii) relevant service provider (which encompasses: authorised payment institutions, small payment institutions, registered account information services provider and electronic money institutions. See Section 2 of the Supervisory statement 6/24 – Operational resilience: Critical third parties to the UK financial sector: **www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-supervisory-statement**.

[3] Financial Policy Summary and Record – October 2021: **www.bankofengland.co.uk/financial-policy-summary-and-record/2021/october-2021.**

financial system (hereafter referred to as a systemic third party service. This and other terms used in this document are as defined in the regulators' rules and expectations).[4]

The CTP regime aims to reduce the risk of systemic disruption by setting new outcomes-focused requirements on CTPs. These requirements, as set out in the regulators' rules and expectations in supervisory statement (SS)6/24 and other relevant policy documents listed in policy statement (PS) 16/24 – Operational resilience: Critical third parties to the UK financial sector[5], focus on CTPs' operational risk management and resilience capabilities. The focused nature of the regime is also reflected in the regulators' powers (see Section 7). Unlike many of the regulators' existing supervisory regimes, CTPs are overseen in respect of their systemic third party services to firms. This document sets out the approach the regulators take with that oversight.

The regime complements the requirements and expectations for firms on operational resilience, outsourcing and third party risk management.[6] The CTP oversight regime sits alongside these requirements and expectations but does not eliminate, reduce nor replace the accountability of firms, their boards and senior management.

For further background information on how operational disruption may impact the stability of, and confidence in, the UK financial system, see:

- Financial Stability in Focus: The FPC's macroprudential approach to operational resilience;[7] and
- Section 3 of SS6/24 – Operational resilience: Critical third parties to the UK financial sector,[8] which builds on the FPC's macroprudential approach to operational resilience to explain how disruption to a CTP's services could impact the stability of, and confidence in, the UK financial system.

---

[4] The regulators rules for CTPs are set out in the following rule instruments: Bank of England FMI Rulebook: Critical Third Parties Instrument 2024, Bank of England FMI Rulebook: Critical Third Parties Emergency Provisions Instrument 2024, PRA Rulebook: Critical Third Parties Instrument 2024 and FCA Handbook: Critical Third Parties Instrument 2024.
The regulators expectations are set out in the joint SS6/24 – Operational resilience: Critical third parties to the UK financial sector and the Bank/PRA's SS7/24 – Reports by skilled persons: Critical third parties: **www.bankofengland.co.uk/prudential-regulation/publication/2024/november/reports-by-skilled-persons-critical-third-parties-supervisory-statement**. The FCA's equivalent guidance on skilled persons reviews is in the FCA instrument.
[5] Available at: **www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-policy-statement**.
[6] **SS1/21 – Operational resilience: Impact tolerances for important business services**, **SS2/21 – Outsourcing and third party risk management**, and **FCA PS21/3 – Building operational resilience**.
[7] Available at: **www.bankofengland.co.uk/financial-stability-in-focus/2024/march-2024**.
[8] **www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-supervisory-statement**.

2: Our objectives

The Financial Services and Markets Act 2000 (as amended) (FSMA) sets out the statutory basis of the CTP regime.

The regulators share an Overall Objective when overseeing CTPs: to manage potential risks to the stability of, or confidence in, the UK financial system that may arise due to a failure in, or disruption to, the systemic service(s) that a CTP provides to one or more firms. This Overall Objective complements each of the regulators' statutory objectives, set out below.

Bank of England's objectives

The Bank has an objective to protect and enhance the stability of the UK financial system. While advancing this objective, the Bank has a secondary objective to act in a way which facilitates innovation in the provision of financial market infrastructure services (including in the infrastructure used for that purpose) with a view to improving the quality, efficiency, and economy of the services.

Prudential Regulation Authority's objectives

The PRA has two primary objectives:

1. a general objective to promote the safety and soundness of all of the firms it regulates; and
2. an objective specific to the regulation of insurers to contribute to the securing of an appropriate degree of protection for those who are or may become policyholders.

The PRA also has two secondary objectives:[9]

1. to act, so far as is reasonably possible, in a way that facilitates effective competition in the markets for services provided by the firms the PRA regulates when they carry out regulated activities; and
2. subject to aligning with relevant international standards, to facilitate the international competitiveness of the economy of the UK (including in particular the financial services sector through the contribution of PRA-authorised persons) and its growth in the medium to long term. The FCA has a similar objective.

[9] FSMA also requires the PRA to 'have regard' to the need to contribute towards achieving compliance by the Secretary of State with the government's 2050 net-zero emissions target and environmental targets where the exercise of PRA functions is relevant to the making of such a contribution, from 1st January 2025.

Financial Conduct Authority's objectives

The FCA has a single strategic objective to ensure financial services markets function well.

To advance its strategic objective the FCA has three operational objectives:

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

The FCA has a secondary objective of facilitating, subject to aligning with relevant international standards, the international competitiveness of the economy of the UK (including in particular, the financial services sector) and its growth in the medium to long term. As previously noted, the PRA has a similar secondary objective.

Alongside these objectives, and where compatible with its consumer protection and integrity objectives, the FCA also has a duty to discharge its general functions in a way which promotes effective competition in the interests of consumers[10].

[10] FSMA also requires the FCA to 'have regard' to the need to contribute towards achieving compliance by the Secretary of State with the government's 2050 net-zero emissions target and environmental targets where the exercise of FCA functions is relevant to the making of such a contribution, from 1st January 2025.

3: Criteria for identifying potential critical third parties and recommending them to HM Treasury for designation

This chapter sets out the regulators' approach to identifying and recommending potential CTPs to HMT for designation. It includes the criteria the regulators consider when assessing whether to recommend a third party to HMT for designation; and the sources of data and information used to support this. The regulators' approach will evolve over time.

HMT may designate a third party that provides services to firms as a CTP. HMT may only exercise this power if, in its opinion, a failure in or disruption to the provision of the services that the third party provides (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system.

Designation decisions, therefore, ultimately lie with HMT. HMT must consult each of the regulators before designating a third party as a CTP. In practice, the regulators recommend to HMT which third parties they consider to have met the statutory test for designation. This is based on the regulators' analysis of relevant data and information. HMT undertakes its own analysis to determine whether a third party should be designated. It is also possible for HMT to designate a third party as a CTP without a recommendation from the regulators.

This chapter should be read alongside Critical Third Parties – HM Treasury's Approach to Designation,[11] which outlines HMT's approach and end-to-end process for designating CTPs; describes how HMT communicates its decisions to designated CTPs; and outlines the Designation Regulations process.

Intended scope of the CTP regime

The statutory test for designation as a CTP in section 312L FSMA is designed to only capture those third parties whose provision of services (either individually or, where more than one service is provided, taken together) could, in the event of a failure or disruption, threaten the stability of, or confidence in, the UK financial system. CTPs are therefore expected to account for a small number and percentage of those third parties providing services to

[11] Available at: www.gov.uk/government/publications/critical-third-parties-hm-treasurys-approach-to-designation.

firms.[12] This is in line with the original intent of the CTP regime as articulated by the Bank's Financial Policy Committee.[13]

Assessing whether to recommend a third party to HM Treasury for designation as a CTP

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

- the materiality of the services provided by the third party to the delivery, by any person, of essential activities services or operations[14] (wherever carried out), and
- the number and type of firms to which the third party provides services (referred to in this document as 'concentration').

The regulators consider these factors as part of their assessment when recommending a third party to HMT for designation as a CTP as well as any other factors that are relevant to identifying whether a third party meets the statutory test for designation.

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

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

Concentration

As set out above, when deciding whether to designate a third party, HMT must consider the 'number and type' of firms to whom the third party provides services. The regulators' analysis considers the use of a third party's services by firms across the financial system as a whole and, where relevant, within specific parts of the financial system. The regulators also take into account the extent to which any of the firms that receive services from a third party are systemically important. This means that the regulators' assessment of concentration looks

---

[12] See paragraph 1.7 of Critical Third Parties – HM Treasury's Approach to Designation: **www.gov.uk/government/publications/critical-third-parties-hm-treasurys-approach-to-designation**.
[13] Available at: **www.bankofengland.co.uk/-/media/boe/files/financial-policy-summary-and-record/2021/july-2021.pdf**.
[14] As per section 312L(7) FSMA.

both at concentration in absolute terms, ie the total number of firms that rely on a given third party service provider's services, as well as the relative systemic significance of those firms.

As noted in the Final report on enhancing third party risk management and oversight – a toolkit for financial institutions and financial authorities (Financial Stability Board third party risk (TPR) toolkit),[15] concentration in the provision of third party services to firms does not automatically pose systemic risks, nor is it inherently or invariably problematic. However, in line with the comments of the FPC in its Q2 2021 Financial Policy Summary and Record,[16] the greater the share of the financial sector relying on a third party, the greater the risk to the UK financial system in the event of a failure in, or disruption to, the services that the third party provides.

Materiality

The regulators' assessment of materiality considers whether there are any channels through which a third party's services to firms could create, amplify or spread risks to the financial system via the financial services that these third party services support. The regulators' methodology builds on UK and international regulatory publications that define systemic risk (and subsets thereof, such as systemic cyber risk).[17]

The regulators' assessment of the systemic materiality of a third party's services to firms for the purposes of identifying potential CTPs is informed by, but may differ from, the way individual firms assess the materiality of their outsourcing and third party (OATP) arrangements. The fact that an individual firm considers the services it receives from a third party as material for its operational resilience does not automatically render these services systemic for the purposes of the regulators' materiality assessment. The regulators' rules refer to those services provided by a CTP which could affect the stability of, or confidence in, the UK financial system as 'systemic third party services'.[18]

---

[15] Available at: **www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/**.
[16] Available at: **www.bankofengland.co.uk/-/media/boe/files/financial-policy-summary-and-record/2021/july-2021.pdf**.
[17] These include the Bank's **Financial Stability Strategy**; Bank's 2017 **Financial Stability Report**, which discusses the nature of systemic cyber risk; The European Systemic Risk Board's 2020 report on **Systemic Cyber Risk**; tools for identifying 'systemic third party dependencies' in the FSB TPR Toolkit; and FPC's macroprudential approach to operational resilience.
[18] 'Systemic third party services' is defined in the regulators' rules as 'services provided by a CTP to one or more firms a failure in, or disruption to, the provision of which (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system.'

The FPC's macroprudential approach to operational resilience[19] identifies a number of 'macro vulnerabilities' which may be present in a third party's services to firms and therefore relevant to the regulators' assessment of the systemic materiality of these services. These include, but are not limited to:

- **interconnectedness:** a multitude of complex interconnections, including those created by outsourcing and third party relationships, increase the likelihood that operational disruptions have knock-on effects, including on financial stability or confidence in the financial system. In assessing the potential for contagion to the financial system following a third party service disruption, the regulators take into account the FPC's analysis of vital financial services (set out in Financial Stability in Focus: The FPC's macroprudential approach to operational resilience)[20] and assess the ability of these services to transmit systemic disruption, depending on how interconnected they are within the financial system; and
- **the speed of transmission** of an operational disruption may also affect its impact on the financial system. Therefore, impact tolerances, including those set by the FPC, also inform the regulators' view on the extent to which a third party's service might be deemed systemic.

The regulators may treat a group of connected services provided by the same service provider to firms as a single systemic third party service if they consider that their disruption or failure could, when taken together, threaten the stability of, or confidence in, the UK financial system.[21] Where a systemic service is made up of a group of services, the regulators' rules apply to these individual services to the extent that they feed into or underpin the systemic service.

Other relevant factors

When identifying potential CTPs, the regulators propose to take into account all other relevant factors that could affect whether a failure in, or disruption to, a third party's services could threaten the stability of, or confidence in, the UK financial system. Such factors are discussed in greater length in section 3 of SS 6/24, which explores how a CTP could have such an effect on stability or confidence in the UK financial system.

One such factor that may be taken into account is the availability, or absence, of a substitute or contingency of a third party's services. For example:

[19] Available at: www.bankofengland.co.uk/financial-stability-in-focus/2024/march-2024.
[20] Available at: www.bankofengland.co.uk/financial-stability-in-focus/2024/march-2024.
[21] In accordance with section 312L(2) FSMA.

- the lack of viable alternative providers for one or more services, or the lack of capacity of these alternative providers; or
- the potential difficulties (including risks) that may arise when trying to migrate certain services in a timely manner from one third party to another or (if applicable) back in-house.

Another factor is whether the third party (including persons in its supply chain) has direct access to firms' assets (as defined in the regulators' rules) as a result of the services it provides. Such access may create, contribute to or increase the potential for systemic risk. This can occur if an event impacting the third party's operations, such as a cyber-attack, create risks to the confidentiality, integrity, authenticity or availability of assets belonging to the firms it provides services to (as noted in the definition of a CTP operational incident in the regulators' rules).

Services already subject to oversight, regulation or supervision

The regulators do not intend to recommend certain third parties for designation as CTPs if the services they provide to firms are already subject to regulation and supervision focused on the resilience of that service in the UK. Such regulation and supervision could be by the other applicable regulator(s) or, in some instances, other authorities. In assessing whether to exclude a given third party from being recommended for designation as a CTP, the regulators look at the regulatory and supervisory arrangements for each of the systemic third party services it provides rather than automatically excluding the entire third party entity from consideration.

In particular, the regulators do not usually recommend third parties that: (i) provide systemic third party services to firms and that meet the criteria for designation as a CTP; but (ii) are already subject to authorisation, regulation, supervision and/or oversight by the PRA, Bank and/or the FCA with respect to the operational resilience of those services. The regulators also exclude firm/intra-group service providers that only provide services to firms in their group from being recommended for designation, irrespective of whether the service providers are authorised, designated (under a regime other than the CTP regime), regulated or supervised on a solo-regulated or dual-regulated basis.

The regulators are also unlikely to recommend a third party providing services to the UK financial system where its services are subject to regulation and oversight by other regulators that deliver comparable outcomes to the CTP oversight regime in relation to the resilience of the service in the UK. For example, sectors that fall under the UK National Infrastructure Resilience Framework are already expected to adopt core principles designed to strengthen the UK's resilience to civil contingency risks.

The regulators use available information-sharing gateways and may create or enhance bilateral and multilateral cooperation with relevant regulators to ensure appropriate cooperation and information-sharing relating to these service providers.

Sources of data and information

The regulators plan to consult on a new policy for OATP data collection.[22] Data provided by firms under the proposed OATP data collection rules is one of the main but not sole source of data to support the identification of potential CTPs. Over the past few years, the regulators have also undertaken ad-hoc data collections relating to firms' OATP arrangements. Data collected in this way continues to inform the regulators' recommendations for designation until the proposed OATP register is operational.

The regulators may also take into account or cross-refer to data and information from other sources, such as material outsourcing notifications and other supervisory intelligence.

The regulators' horizon scanning may also enable them to identify and monitor third parties that may not meet the criteria for designation as a CTP at a given time but could do so in the future. For instance, where the third parties' service provisions have expanded and play a greater role in particular firms, or become more widely used.

Communication with CTPs about their designation and systemic third party services (including periodic reviews)

Under FSMA, the regulators have the power to make rules imposing duties on CTPs in connection with their provision of services to firms. As discussed in PS16/24, the regulators have limited the scope of all their rules (except CTP Fundamental Rule 6) to a CTP's provision of systemic third party services. When recommending to HMT that it designates a third party as a CTP, the regulators expect to indicate to HMT which of the third party's services to firms have been identified as potentially having a systemic impact on UK financial stability or confidence in the UK financial system. Potential CTPs are able to make representations about these services to HMT prior to any decision on designation.[23]

If HMT decides to designate a third party as a CTP, it writes to the prospective CTP to communicate its decision prior to publishing its Designation Regulations. The prospective

[22] Incident and Outsourcing and Third Party Reporting: **www.fca.org.uk/publications/corporate-documents/regulatory-initiatives-grid**.
[23] See section 312L(4)(b) FSMA and Critical Third Parties: HM Treasury's Approach do Designation: **www.gov.uk/government/publications/critical-third-parties-hm-treasurys-approach-to-designation**.

CTP is also notified of the services which the regulators and HMT consider to be systemic third party services at the point of designation.

The regulators periodically review whether, in the regulators' opinion, a CTP continues to meet the criteria for designation and update HMT accordingly. Such reviews apply the same assessment criteria as those used in recommending a new CTP for designation by HMT at the time of that review. The regulators intend to use all relevant data and information sources. These include data and information received from firms and CTPs, as well as those obtained from CTP oversight activities, such as notifications from CTPs of significant changes in the systemic third party services provided. Any decision to remove the designated status of a CTP is a matter for HMT.

Following each of these periodic reviews, the regulators will, where relevant:

- recommend to HMT that it removes the designation of any CTP which they consider no longer meets the statutory test for designation; or
- for those CTPs which continue to meet the criteria for designation, flag whether the review has highlighted any changes in the systemic third party services provided. For instance, potential new systemic third party services, or formerly systemic third party services which may potentially no longer meet the definition.

4: Our approach to advancing our objectives

To advance the regulators' objectives, the approach to CTP oversight follows several key principles.

Judgement-based and evidence led

The oversight teams reach judgements on the risks that disruption to a CTP's systemic third party services pose, and the ways these are mitigated, based on evidence and analysis. The regulators use information from a broad range of sources, including CTPs, firms, the regulators' own sectoral analysis and relevant other authorities.

The regulators' strategies and judgements are subject to regular internal review by those independent from overseeing the CTP in question. The regulators major judgements and decisions involve their most senior and experienced staff and directors.

Forward-looking

The regulators' oversight approach is forward-looking. We assess CTPs not just against current risks, but also against those that could plausibly arise in the future. Where it is judged necessary, the regulators seek to intervene at an early stage to reduce the likelihood of risks crystalising.

To support this, and in line with the Fundamental Rule 6, CTPs should be open and straightforward in their dealings with the regulators, taking the initiative to raise issues of possible concern at an early stage.[24] The regulators will respond proportionately, ensuring trust can be fostered on both sides.

Proportionate and focused on key risks

The regulators focus their oversight on the issues that pose the greatest risk to the regime's Overall Objective, and do so in a proportionate manner. As outlined further in Section 6 below, the regulators' risk assessment takes into account both the gross risk and any mitigating factors.

Outcomes-focused

The regulators' oversight approach is intended to be outcomes-focused. The regulators assess CTPs' compliance with the outcomes-focused rules and expectations and will move

[24] Critical Third Parties Part 3.6 and 3.7, Bank of England FMI Rulebook and corresponding Fundamental Rule in the PRA and FCA Instruments.

quickly to take action, including the use of statutory powers, in order to further the regime's Overall Objective.

Transparency

The regulators aim to be as transparent as possible when engaging with a CTP and when using legal powers. The regulators are clear with CTPs and individuals about their oversight observations, work and priorities.

Integrated and coordinated

The regulators ensure their oversight teams work closely to share information, reach robust decisions and provide consistent messages. As outlined further in Section 7, the regulators coordinate with relevant domestic and international authorities and regulators.

5: Implementation across the regulators

Coordination between the regulators forms the foundation of the approach to CTP oversight.

Shared responsibility for oversight of CTPs between the PRA, Bank and FCA is an important aspect of the regime. The regulators share the common Overall Objective when overseeing CTPs, and must also comply with their own statutory objectives. Furthermore, the regulators have a statutory duty to coordinate the exercise of their respective CTP functions under section 312U of FSMA and to consult each of the other relevant regulators before exercising any of their CTP statutory powers.[25]

A joint CTP Consultation and Coordination Forum (CCF) is one of the primary means by which the regulators co-ordinate the exercise of their respective functions conferred under the CTP regime. Coordination is further facilitated by common memberships across the FCA Board, the PRA's Prudential Regulation Committee[26] and the Bank's Financial Market Infrastructure Committee[27], which allows discussions of areas of overlap between the regulators at a senior level. Further details on the CCF and the regulators' approach to coordinating their oversight of CTPs is described in a Memorandum of Understanding (MOU).[28]

The regulators expect to conduct oversight activities in a manner that minimises the compliance burden on CTPs while also enabling the regulators to further their respective objectives (though the regulators may in some circumstances still act on an individual basis if it is necessary or appropriate). The regulators intend to coordinate oversight activities in areas including:

- reviews of self-assessments (interim and annual), and any supporting documentation provided by the CTP (certifications, standards etc);
- regular and ad-hoc meetings with the CTP;
- deep dive and thematic reviews (including skilled persons reports);
- use of powers, including information gathering and referrals to enforcement;
- participation in incident management playbook exercises (including any feedback provided to the CTP after the exercise);
- consideration of incident reports and follow-up actions; and

25 Available at: **www.legislation.gov.uk/ukpga/2000/8/section/312U**.
26 Available at: **www.bankofengland.co.uk/about/people/prudential-regulation-committee**
27 Available at: **www.bankofengland.co.uk/about/people/fmi-committee**.
28 Available at: **www.gov.uk/government/publications/memorandum-of-understanding-between-the-bank-of-england-fca-and-pra**, as required by: **www.legislation.gov.uk/ukpga/2000/8/section/312V**.

- engagement with other UK authorities and non-UK financial regulators.

The regulators share information as set out in the MOU to ensure effective coordination and to minimise the need for CTPs to share information with each regulator separately. The regulators also seek, as far as possible, to deliver consistent messages to CTPs and to agree a single set of actions for each CTP, where this furthers each regulator’s objectives.

6: Identifying risks to the financial system

The intensity of our oversight activity may vary across CTPs. Our oversight activity reflects our judgement about the potential impact of disruption in a CTP's systemic third party services on the financial system and on the advancement of our objectives.

Focus on CTPs' services to firms

Although HMT designates CTPs at the entity level, the oversight regime for CTPs applies in relation to the services that CTPs provide to firms. With the exception of CTP Fundamental Rule 6, the regulators' rules only apply in relation to a CTP's provision of systemic third party services to firms.[29] Section 3 explains how these systemic third party services are identified during the process culminating in the designation of a third party as a CTP by HMT, and reviewed regularly thereafter. For further details on the definition of systemic third party services, see Section 4 of SS6/24.[30]

While the majority of the regulators' oversight focuses on a CTP's systemic third party services, the regulators may also look at non-systemic third party services that a CTP provides to firms if appropriate. For instance, where there are interconnections or common dependencies between systemic and non-systemic third party services (eg where both services are dependent on the same technology and Key Nth Party Providers). The regulators may also use their information-gathering powers under section 312P of FSMA to request information from a CTP about a service it provides to firms that is not considered a systemic third-party service at the time of the information request, but could become so in the future due to rapid adoption among firms.

Our risk assessment framework

The regulators take a structured approach when forming judgements on risks. A risk assessment framework is used to assess the risk posed to a CTP and its systemic third party service(s) – see Figure 1.

The risk assessment framework allows the regulators to assess the gross risk to the delivery of systemic third party service(s) provided by the CTP either from the external environment or internally because of the way the service is delivered by the CTP. The framework then considers mitigating factors a CTP may have put in place to offset these gross risks. When

[29] Critical Third Parties Part 3, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.
[30] Available at: www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-supervisory-statement.

taken together, this assists the regulators in making an assessment of the net risk that any given CTP and the delivery of its systemic third party services could pose to the stability or confidence in the UK financial system.

Figure 1: The CTP risk assessment framework

Gross risk		Mitigating factors	
External environment	Internal risk	Risk governance, management and controls	Operational resilience

External environment

Any assessment of the risks posed by a CTP's provision of systemic third party service(s) requires consideration of the external environment in which the CTP operates. External environment refers to any external factors that could pose a threat to a CTP's ability to deliver its systemic third party services and meet their oversight obligations. The regulators' assessment includes the cyber-security threat landscape; the evolving technology landscape (including trends in the adoption of technology by firms); risks to a CTP's physical infrastructure (such as from climate change, natural disasters and disruption to the energy supply). The regulators consider relevant risks from general economic, and market conditions and the political, geopolitical, legal, and regulatory landscape, as well as considering potential interconnections between these external environment risks – for instance, between the geopolitical and cyber-security threat landscape.

The regulators draw on wider analysis, including the views of the FPC and sectoral analysis to understand key market developments and information directly from firms and CTPs. The regulators also consider actions taken by other domestic and international authorities that may materially affect the systemic third party services provided by CTPs and, subject to appropriate cooperation and information-sharing arrangements, information and intelligence from other regulators and authorities.

Internal risk

Internal risks are risks that arise from the way a CTP delivers its systemic third party service(s). The regulators' assessment of internal risks may include, but are not limited to, the consideration of risks arising from:

- a CTP's business model, as it relates to its delivery of systemic third party services;
- a CTP's organisational (including group), and ownership structure. For example, a CTP merging or acquiring another company and combining services. In this case, we expect CTPs to have sufficient controls and process in place to manage the risk;
- dependencies on, and interaction with, the CTP's wider group;
- specific developments, such as large-scale transformation projects that may affect a CTP's systemic third party services;

- supply chain dependencies, including but not limited to:
  - the length and complexity of the supply chain; or
  - concentration and single-points-of-failure on Key Nth Party Providers, geographic locations etc;
- people, including insider threats and key-person dependencies; and
- a CTP's financial viability and financial resilience.

Risk governance, management and controls

A CTP should have robust frameworks for management of all risk types, including both internal and external risks.[31] Robust risk management frameworks enable a CTP to effectively identify, measure, monitor, manage and report risks in relation to their systemic third party services. The policies, procedures and controls in place should be comprehensive and scale with the complexity of these services.

Governance arrangements play an important role in a CTP's approach to risk management.[32] The regulators' focus on systemic third party services means that the regulators consideration of governance arrangements differs from that of firms. For example, the regulators require CTPs to establish clear roles and responsibilities at all levels of its staff who are essential to the delivery of a systemic third party service. The regulators also examine whether internal communication at the CTP is effective and consistent with prudent risk management. The regulators place strong emphasis on the timely escalation of issues and risks, in order for relevant staff at the CTP (including specialist teams, and, if appropriate, senior management the governing body) to take action if required.

The regulators understand that each systemic third party service may present different risks to our objectives and, while many of these are operational in nature, a CTP is required to manage financial risks relevant to its ability to deliver systemic third party services and comply with its duties under the CTP oversight regime. In assessing this, the regulators consider relevant financial information, some of which may be in the public domain in the case of CTPs that are listed or belong to a listed group. This may include how a CTP manages risks to its financial viability and maintains sufficient financial resources to support the delivery of a systemic third party service during transitional arrangements with clients in the event of termination.[33]

The regulators take a risk-based approach to oversight and focus their attention on the areas that present the most risk to their objectives. Central to the regulators' rules and expectations are dependency and supply chain risk management, technology and cyber resilience, and

[31] Critical Third Parties Part 4.4, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.
[32] Critical Third Parties Part 4.3, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.
[33] Critical Third Parties Part 4.11, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.

change management.[34] Assessing the extent to which CTPs and their systemic third party services comply with and meet these requirements forms a key part of our oversight of this risk element.

A CTP must identify and manage risks to its supply chain that could affect its ability to deliver a systemic third party service. When assessing a CTP's approach to supply chain risk management, the regulators examine whether a CTP has performed appropriate due diligence before entering or significantly changing contractual arrangements and ensure lessons learned from disruptions are appropriately reflected in risk and incident management processes.

Technology and cyber resilience is a particularly important requirement given the role of technology in the provision of many systemic third party services and the numerous ways in which a CTP can be compromised. A CTP is required to have processes and measures in place to identify, assess, mitigate, measure and manage technology and cyber risks. The regulators seek evidence of the effectiveness of these measures as well as understanding a CTP's capability to identify, assess and remediate vulnerabilities.

The scale and number of changes made to systemic third party services varies between CTPs. However, all CTPs must have an effective approach to dealing with changes to its systemic third party services. When assessing change management, the regulators consider whether changes are appropriately risk-assessed. This is especially important for significant changes that present a sizeable risk to the delivery of a systemic third party service.

The regulators expect CTPs to use mapping to enhance their risk management, including through identifying essential resources in the supply chain and assessing associated risks and any external dependencies and interconnections. Mapping should also help CTPs assess risks in the supply chain of its systemic third party services, allowing steps to be taken to further enhance the resilience of these services[35].

Operational resilience

Operational resilience refers to the ability of CTPs and the financial sector as a whole to prevent, adapt, respond to, recover from, and learn from, operational disruptions. The regulators expect to see evidence that a CTP's systemic third party service(s) are sufficiently resilient so that CTP operational incidents do not negatively affect the stability of, or confidence in, the UK financial system.

Key to the regulators' assessment of operational resilience is how a CTP carries out scenario testing and demonstrates it can continue to provide each systemic third party service within

[34] Critical Third Parties Part 4.5 – 4.8, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.
[35] Critical Third Parties Part 4.9, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.

its maximum tolerable level of disruption in the event of a severe but plausible disruption.[36] The regulators pay close attention to how CTPs have assigned the tolerance for disruption and sufficiently tested against it with a well-thought-out and comprehensive scenario testing programme. We particularly scrutinise scenario selection and calibration, and expect mapping, threat intelligence and prior CTP operational incidents to be included among the ways a CTP informs its scenario testing.[37] In response to a new or emerging risk, the regulators may request additional scenario tests. These scenarios may be identified in collaboration with:

- firms;
- collective incident response frameworks;
- non-UK financial authorities;
- standard-setting bodies and other international organisations;
- non-financial UK authorities; and
- industry experts.

Appropriate incident management is an important operational mitigant. CTPs should have comprehensive, well-tested and up to date response and recovery measures.[38] As part of this, CTPs should also consider the contingencies available should their core delivery mechanisms fail. The regulators assess whether a CTP has an appropriate range of these measures, and evidence of their effectiveness, including continual improvements as a result of testing, exercises and incidents.

An incident management playbook complements these measures by ensuring CTPs understand how to communicate and support the regulators and firms during CTP operational incidents.[39] After a CTP exercise, the regulators may follow-up with the CTP to ensure revisions to the playbook and lessons learnt are fully embedded. If justified, the regulators may direct a CTP to carry out an incident management playbook exercise, or a similar exercise earlier or more frequently than biennially.[40] For instance, to assess whether remediation following a CTP Operational Incident has been implemented appropriately, or ahead of a major change management programme. The regulators may observe selected incident management playbook exercises to:

---

[36] Critical Third Parties Part 5.2, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.
[37] Critical Third Parties Part 5.3, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.
[38] Critical Third Parties Part 4.10 (1), Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.
[39] Critical Third Parties Part 5.4, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.
[40] Critical Third Parties Part 5.5, Bank of England FMI Rulebook and corresponding rules in the PRA and FCA Instruments.

- improve their own capabilities to coordinate with CTPs, firms during a CTP operational incident that affects the financial sector eg by invoking the Authorities' Response Framework (ARF); and
- identify ways to improve communication with CTPs and affected firms during CTP operational incidents.

To promote regulatory and supervisory interoperability, the regulators may invite non-UK financial regulators and UK non-financial regulators, public, and authorities that carry out similar functions or have overlapping mandates over CTPs to observe incident management playbook exercises. The regulators will give a CTP advance notice if they intend to observe an incident management playbooks exercise, either alone or with another authority.

Box 1: The regulators' approach to incident management

> Once the regulators receive an initial incident report from a CTP, it is triaged and the most appropriate response is considered on a case-by-case basis. When doing this, the regulators may coordinate and share information with other authorities, for instance, HMT, non-UK financial authorities and UK non-financial authorities (including the National Cyber Security Centre if the incident is a cyber-incident), subject to appropriate information-sharing arrangements, such as memoranda of understanding or a statutory information-sharing gateway.
>
> In the event of an incident or threat that could cause major disruption to financial services, the regulators may invoke the ARF. The joint framework is owned and governed by senior representatives from across the Bank (including the PRA), the FCA and HMT. Invoking the ARF allows the three authorities to closely coordinate their response while considering any impacts to their own statutory objectives.

Having appropriate arrangements and provisions in place to respond to a termination of any of its systemic third party services is also a key mitigant and reduces risks to the regulators' objectives by lessening the potential impact of firms' important business services being disrupted. The regulators review these arrangements on a periodic basis and pay close attention to actual and hypothetical examples which illustrate how CTPs support firms in the event of termination of a CTP's service(s).

7: Oversight activity

This section describes how the regulators oversee CTPs in practice, including use of tools and legal powers. The regulators' oversight activity is focused on identifying or addressing risks and is proportionate to the potential impact that disruption in a CTP's systemic third party service(s) could have on the stability of, or confidence in the UK financial system.

The CTP oversight cycle

A typical CTP oversight assessment period, or oversight cycle, lasts 12 months and is centred around an internal assessment meeting between the regulators known as an Annual Review. In these meetings the regulators:

- discuss the key risks a CTP poses to the regime's Overall Objective based on developments over the preceding 12 month oversight cycle, including oversight activities, CTP Operational Incidents (if applicable), recent or planned major change initiatives and engagement with other authorities; and
- agree the oversight strategy for the upcoming 12 months, including planned oversight activities and actions the CTP will be requested to take, such as specific testing or remediation.

The oversight activities and actions referred to above are additional to those that every CTP is required to complete under the regulators' rules, such as the submission of the annual self-assessment, regular scenario testing and biennial incident management playbook exercises.[41]

Annual Reviews include input and reviews from staff at the regulators not directly involved in the day-to-day oversight of the CTP. This includes legal, policy, relevant subject matter experts and independent advisers within the regulators. Senior management across the regulators also rigorously scrutinise Annual Reviews.

There is a clear and direct link between the risks identified in the Annual Review and the actions the regulators request a CTP take throughout the annual CTP oversight cycle. The regulators focus on the most significant risks identified, and the steps that should be taken to reduce risks to the Overall Objective. For example, if the regulators have identified issues in a CTP's risk management framework for one or more systemic third party services, or its incident management playbook, the regulators may request the CTP make changes to rectify these issues.

[41] Following the first playbook exercise which must be carried out within 12 months of designation by HMT.

Following the Annual Review, the regulators write to the CTP clearly outlining the risks that are of greatest concern and where it is expected that the CTP takes risk management, risk mitigation or remediation actions.

Box 2: First year of CTP oversight

> The regulators' interaction with a newly designated CTP ahead of the first Annual Review generally looks different to the regular oversight work the regulators' conduct. It focuses on helping to build a picture of a CTP's resilience, with the aim of forming an initial view of the risks it poses to the Overall Objective. This is reflected in the meetings and oversight activities conducted.
>
> The interim self-assessment is a key component in this process and provides the regulators with an early indication of the extent to which a CTP is able to meet the CTP duties at the point of designation. This helps the regulators ensure subsequent oversight is risk-based, resource efficient and targeted.
>
> The regulators also acknowledge that the interim self-assessment is likely to be less developed than subsequent, annual self-assessments and that a CTP may be unable to demonstrate full compliance with all the requirements in the rules at the time of submission.

The regulators expect the top layer of decision-making responsible for the delivery of systemic third party services to firms to respond setting out how they will address concerns and requested actions in our Annual Review letter.[42] The regulators monitor a CTP's execution of these actions using the oversight tools described below.

On a periodic basis the regulators also consider whether a CTP and its systemic third party service(s) continue to meet the criteria for designation by HMT. In line with Fundamental Rule 6, the regulators expect to be informed of significant changes to a CTP or its systemic third party service(s). The regulators assess whether these changes, including changes to a CTP's corporate structure, may affect whether a CTP still meets the statutory criteria for designation and make recommendations to HMT accordingly.

CTPs may sometimes disagree with the regulators' judgements. This is inherent given the tensions between the public and private interest. The regulators generally discuss issues with CTPs as part of reaching our decisions and carefully consider any representations made, not least to ensure that decisions are made on the basis of all the relevant evidence. To enable this, the regulators expect CTPs to interact in an open and co-operative manner, as noted in

[42] As noted in Operational Risk and Resilience Requirement 1 (Governance), this layer could be the CTP's governing body or a committee thereof; its senior management; or a specialised committee, individual, or group.

Fundamental Rule 6.[43] However, CTPs should not approach their engagements as a negotiation.

Engagement with CTPs

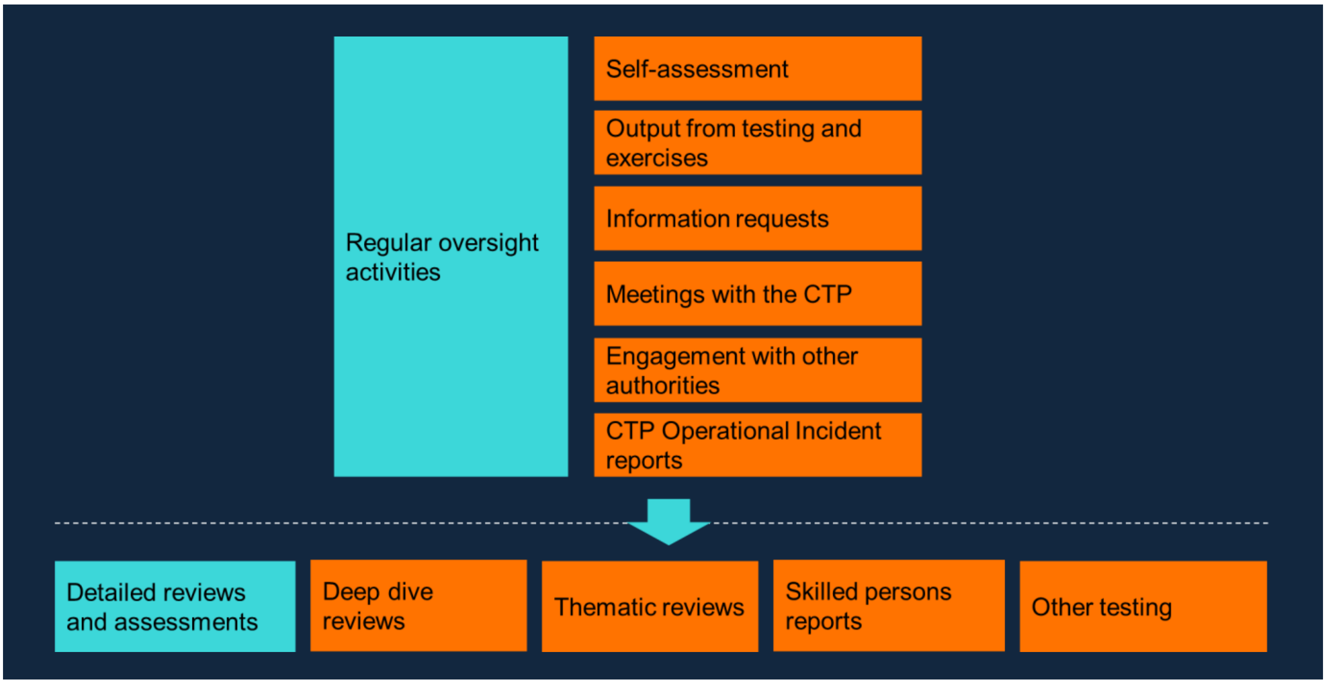
The regulators take a risk-based approach to the assessment of CTPs. Certain assessment activities are fundamental to the oversight approach and are used regularly for all CTPs to form a view of risks. These activities include the review of a CTP's self-assessment and testing outputs, analysis of regular and ad-hoc data and information, meetings with CTP staff, and engagement with other authorities. In addition, the regulators may carry out further assurance via 'deep dive' examinations, thematic reviews, skilled person reports or other relevant assurance, exercising or testing activities.

Figure 2: CTP oversight cycle

The regulators usually engage with a CTP via its appointed employee(s) or member(s) of its governing body. However, if appropriate, the regulators may also engage with other CTP employees or members of its governing body, such as specialists in a specific area. Where appropriate, the designated point of contact should engage with other group companies not designated as CTPs, but which support the delivery of systemic third party services, or a CTP's compliance with the CTP duties on the regulators' behalf.

[43] Critical Third Parties Part 3.6 and 3.7, Bank of England FMI Rulebook and corresponding Fundamental Rule in the PRA and FCA Instruments.

Figure 3: Oversight activities and assessments



Self-assessment

Central to the oversight approach is the annual self-assessment through which CTPs set out their analysis of how they have complied with the regulators' rules and expectations. It is an important test of a CTP's ability and willingness to demonstrate their understanding of, and commitment to the regime and its objectives.[44]

Self-assessment does not mean self-regulation. Self-assessments play an important role in helping the regulators assess the resilience of systemic third party services and the key risks to the regime's Overall Objective. They are viewed as an indication of a CTP's own risk management and resilience capability. The regulators use them to inform the oversight strategy for a CTP and identify areas to prioritise for further work in the forthcoming year. While the information requirements for the self-assessment as set out in the SS 6/24 are identical, an interim self-assessment seeks to fulfil a unique objective: to provide the regulators with an early indication of the extent to which a CTP is able to meet the CTP duties at the point of designation. The regulators expect CTPs' self-assessments to evolve following engagement and throughout the period they are subject to regulatory oversight.

Testing

Testing is a key element of the regulators' oversight approach. This includes not only scenario testing, as outlined in Section 6, but also other forms of internal testing conducted

[44] Critical Third Parties Part 6, Bank of England FMI Rulebook and corresponding Fundamental Rule in the PRA and FCA Instruments.

by a CTP that is not explicitly mandated by the regulators' rules and may be used to demonstrate compliance with the regulators' rules.

As part of the self-assessment review process, the regulators assess a CTP's approach to testing and assurance. The approach, type, scope, frequency, participation, and mode of testing will vary between CTPs, but should be sufficient to demonstrate compliance with the risk and resilience outcomes of the CTP regime. The regulators use outputs and results from testing to form a view of CTPs' resilience. The regulators also assess a CTP's lessons learned culture and whether these are fully embedded to support the ongoing improvement of its resilience.

Exercising

Conducting an exercise allows a CTP to assess its ability to respond, recover and support firms and the wider financial system in the event of a CTP operational incident. The incident management playbook is one such example. Unlike internal testing, exercises involve external stakeholders such as CTP customers, and help CTPs manage risks to the stability of, or confidence in, the UK financial system, by interacting and collaborating with the financial sector. Exercises also provide the regulators with a view of how CTPs manage potential systemic risks.

Regular exercises enable a CTP to adopt a continuous improvement model through exercising, evaluating, improving, and re-exercising. The regulators expect exercising to be an important feature of the oversight approach and an important aspect of the work conducted by CTPs to demonstrate how they can deliver a resilience outcome.

The regulators' oversight approach includes assessing how CTPs design and run exercises, as well as following-up on actions taken to remediate any identified shortcomings. For exercises to be effective the regulators expect CTPs to conduct them with a representative sample of their customers. To maximise the benefits of conducting an exercise, a CTP should ensure it receives feedback from external stakeholders. Joint scenario-based exercises, such as the incident management playbook exercise, complement rather than replace sector-wide initiatives.

Ad-hoc and regular information requests

Information the regulators request depends on the nature of a CTP and services (both its systemic third party services and other services associated with 'Persons Connected to a CTP', including group entities). Information requested on a regular basis may include (but is not limited to) service availability data, audit reports, certain internal governance committee papers and data on incidents such as near misses that did not meet the notification threshold. The regulators may also request information in other ways, including by written questionnaire. The regulators may exercise powers under section 165 of FSMA when requesting information.

Meetings

The regulators hold regular and ad-hoc meetings with relevant individuals at CTPs. With whom we meet will depend on the CTPs' organisational structure and type of systemic third party service(s) they provide, but they should include those responsible for the delivery of these services with decision-making powers. The regulators discuss the most appropriate individuals to meet with newly designated CTPs.

Detailed reviews and assessments

The regulators may choose to undertake more detailed assessments and reviews of particular risk areas, for example where oversight work, information received, or an operational incident indicates elevated risk; or where other oversight approach elements have not provided sufficient information to assess.

This further assurance may be conducted via 'deep dive' examinations, which are an in-depth assessment of a particular aspect of a single CTP. For example, an examination related to one of the operational resilience and resilience requirements. Thematic reviews and peer analysis may be used on multiple CTPs to provide a diagnostic tool to highlight where individual CTPs may be outliers relative to peers on a specific topic. Such analysis also provides a view of common sectoral risks that have the potential to impact the stability of the system. As noted in Box 3, these reviews may also be conducted via a Skilled Person. In general, the regulators provide thematic feedback to CTPs following such reviews where it is assessed that sharing the findings is beneficial. The regulators may also ask a CTP to carry out other relevant testing activities, such as additional scenario tests or incident management playbook exercises.

The nature of a review depends on the focus area, but they will typically include an information request and meetings with CTP staff. At the end of the review, the regulators draw conclusions and may discuss with the CTP any follow-up actions that the CTP is requested to take. The regulators may also choose to further validate previously agreed follow-up actions and assess their effectiveness in addressing shortcomings that have been identified.

On occasions where it is judged necessary or helpful to the review, oversight work may have an onsite component. The regulators will attempt to minimise the impact of onsite visits, and every effort is made to avoid duplication of onsite oversight activities. Alongside the immediate oversight team, the regulators may involve internal risk specialists and other technical staff in these assessments.

In addition to the regulators' own reviews, and where their effectiveness can be relied on, there may be times where the regulators may ask CTPs to conduct their own internal reviews or testing of specific areas for submission to the regulators. In some cases, the regulators may also use legal powers to commission a Skilled Persons report, as further set out in

SS7/24: Reports by skilled persons: Critical Third Parties.[45] The regulators already use this tool on regulated firms to examine a range of topics. The use of a skilled persons report does not imply any presumption of wrongdoing or rule breach on a CTP's part in and of itself. Further detail on the regulators' approach to using the section 166 Skilled Person powers can be found in Box 3.

Box 3: Section 166 Skilled persons reports

Skilled Persons reports (under s166 of FSMA) are a tool that the regulators draw on in our oversight of CTPs across all areas of our assessment.

A skilled person could be appointed to produce a report for a series of reasons including:

- (i) diagnostic purposes: to identify, assess and measure risks;
- (ii) for monitoring purposes: to track the development of identified risks, wherever these arise;
- (iii) for preventative action: to limit or reduce identified risks and so prevent them from crystallising or increasing;
- (iv) for remedial action: to allow the regulators to respond to risks when they have crystallised; or
- (v) thematic reviews: where the regulators seek to assess multiple CTPs or systemic third party services and explore sectoral risks or identify outliers relative to peers.

The use of the tool could be prompted by:

- (i) a specific requirement by the regulators for information;
- (ii) an analysis of information undertaken by the regulators;
- (iii) an assessment of a situation by the regulators;
- (iv) expert advice or recommendations received by the regulators; or
- (v) a decision by the regulators to seek assurance in relation to a regulatory submission.

The regulators might choose to obtain a report in circumstances where an enforcement investigation is being contemplated or is underway.

[45] Available at: www.bankofengland.co.uk/prudential-regulation/publication/2024/november/reports-by-skilled-persons-critical-third-parties-supervisory-statement. The FCA's equivalent guidance on skilled persons reviews is in the FCA Instrument.

Engagement with international and other domestic authorities

Some CTPs may be internationally active or headquartered outside of the UK. Given these cross-jurisdiction operations, the regulators expect to engage with international authorities as part of their oversight.

This co-operation contributes to the effective oversight of CTPs regulated in the UK and promotes interoperability with other regimes aimed at managing systemic risks posed by what the FSB TPR toolkit refers to as 'systemic third party dependencies' and 'financial sector critical service providers'.[46] For example, by accepting information from CTPs submitted to other authorities, where it meets the standards and outcomes of the CTP regime. To achieve this, the regulators may:

- ask CTPs for information provided to the authorities responsible for these regimes in other jurisdictions so as to take this information into consideration in their oversight. For example, if the CTP is also designated as a critical ICT third-party service provider under DORA, information provided to its Lead Overseer under Articles 3-6 of the Joint Regulatory Technical Standards on the harmonisation of conditions enabling the conduct of the oversight activities;[47]
- accept incident notifications or reports submitted by CTPs to firms, and/or other authorities, but only if they include the information specified in the regulators' rules for CTP Operational Incidents and section 8 of the SS;
- exchange information relating to CTPs of mutual interest with these authorities; and
- invite relevant authorities to observe CTP Exercises (see Section 6 for more details).

The regulators recognise that there may be legal restrictions on the ability of CTPs to share information provided to other authorities. Consequently, the regulators may seek this information directly from relevant authorities (either alternatively or in addition to requesting it from CTPs) if there are appropriate:

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

The regulators may also seek to share information and consult with international authorities where beneficial to conducting oversight activities.

---

[46] A service provider to financial institutions whose services have been deemed by financial authorities to give rise to a systemic third-party dependency with potential implications on financial stability, including potential systemic risk case of disruption or failure. This is a general concept, and the specific term and definition may differ depending on jurisdictions.
[47] Available at: **www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/joint-regulatory-technical-standards-harmonisation-conditions-enabling-conduct-oversight-activities**.

In addition to seeking cooperation with international authorities, the regulators also engage with other domestic authorities for similar purposes. This includes where additional information is sought to support assessments of a CTP, or in response to cross-sector incidents. See Box 1 for additional detail on the regulators' approach to managing CTP operational incidents. At times, we may also use our perspective on third parties and certain sectors to cooperate with and aid other domestic regulators, where appropriate and permissible to do so.

Using powers in the course of oversight

There may be circumstances where the regulators choose to use statutory powers to assist with risk assessment. Most notably, this includes information gathering powers and powers to commission reports by Skilled Persons on specific areas of interest (under section 165, section 166 and section 166A of FSMA).[48] Such reviews can be undertaken where the regulators seek additional information, an assessment, further analysis, independent expert advice and recommendations, or where assurances are reasonably required in connection with our regulatory functions in respect of CTPs. The regulators may select and appoint a Skilled Person directly, following a transparent and consistent approach to selecting them, or may require the CTP to select and appoint with the Skilled Person directly. The regulators are always regarded as the end user of a Skilled Persons report regardless of the appointment approach taken. Further detail on our approach to using section 166 Skilled Person powers can be found in Box 3 and the regulators' respective policies.[49]

The regulators' rules and expectations apply to and are enforceable against the entity or entities listed in the HMT regulations designating a CTP. However, that entity or entities may rely on other entities or parts of their group for the delivery of systemic third party services to firms or other aspects relevant to their compliance with the CTP duties. As a result, our oversight approach is broader than the designated entity or entities in some key areas: the regulators' information gathering powers in section 312P of FSMA extend to 'Persons Connected to a CTP', which include these group entities. The regulators can therefore request information directly from these entities. Under section 312P(5) of FSMA, the regulators also have the ability to appoint a skilled person in respect of a person connected with a CTP (as defined in section 312P(10) FSMA), including wider group entities of the CTP.

The regulators' other powers include powers of direction, through which the regulators can direct a CTP to do or refrain from doing anything specified in the direction where necessary or expedient for the purpose of advancing any of the regulators' objectives.[50] For example,

---

[48] Section 312P FSMA.

[49] Bank of England SS7/24 – Reports by skilled persons: Critical third parties; and chapters 12 and 13 of the Critical Third Parties Sourcebook in the FCA Handbook.

[50] Section 312N FSMA.

the regulators may require a CTP to undertake remediation actions following the identification of a risk if it is assessed to have the potential to cause harm.

In certain circumstances, the regulators may use powers under section 138A FSMA[51] to grant a waiver or modification to a rule where they are content that the conditions to using that power are met. This includes if the CTP's compliance with that rule would not achieve its intended purpose or outcome.

While the regulators look to CTPs to co-operate in resolving oversight issues, formal powers will be used where considered an appropriate means of achieving the desired oversight outcomes. There is sufficient flexibility for the regulators to tailor requirements specific to the circumstances of a CTP and the nature of their concerns. Consequently, the regulators may choose to deploy formal powers at an early stage and not merely as a last resort.

The regulators consider when and how to use formal powers, and assess the particular facts and circumstances, on a case-by-case basis. In all cases, the regulators are likely to consider a number of factors in connection with the possible deployment of such powers, including:

- the confidence the regulators have that CTPs will respond appropriately to requests without the use of powers; and
- the level of risk we believe the CTP may pose to the stability of, or confidence in, the UK financial system.

In addition to oversight powers, in situations where the regulators consider that a CTP has contravened an applicable regulatory requirement, there are also powers for the regulators to take enforcement action, which may potentially result in public censure and/or other disciplinary measures. For further information please see The Bank of England's Approach to Enforcement[52] and FCA's Approach to Enforcement is in Section 3 of the CTP Policy Statement.[53]

---

[51] As applied to the Bank by paragraph 10A(a) of Schedule 17A to FSMA.
[52] Available at: **www.bankofengland.co.uk/prudential-regulation/publication/2024/january/the-bank-of-england-approach-to-enforcement-statements-of-policy-and-procedure**.
[53] Available at: **www.bankofengland.co.uk/prudential-regulation/publication/2024/november/operational-resilience-critical-third-parties-to-the-uk-financial-sector-policy-statement**.