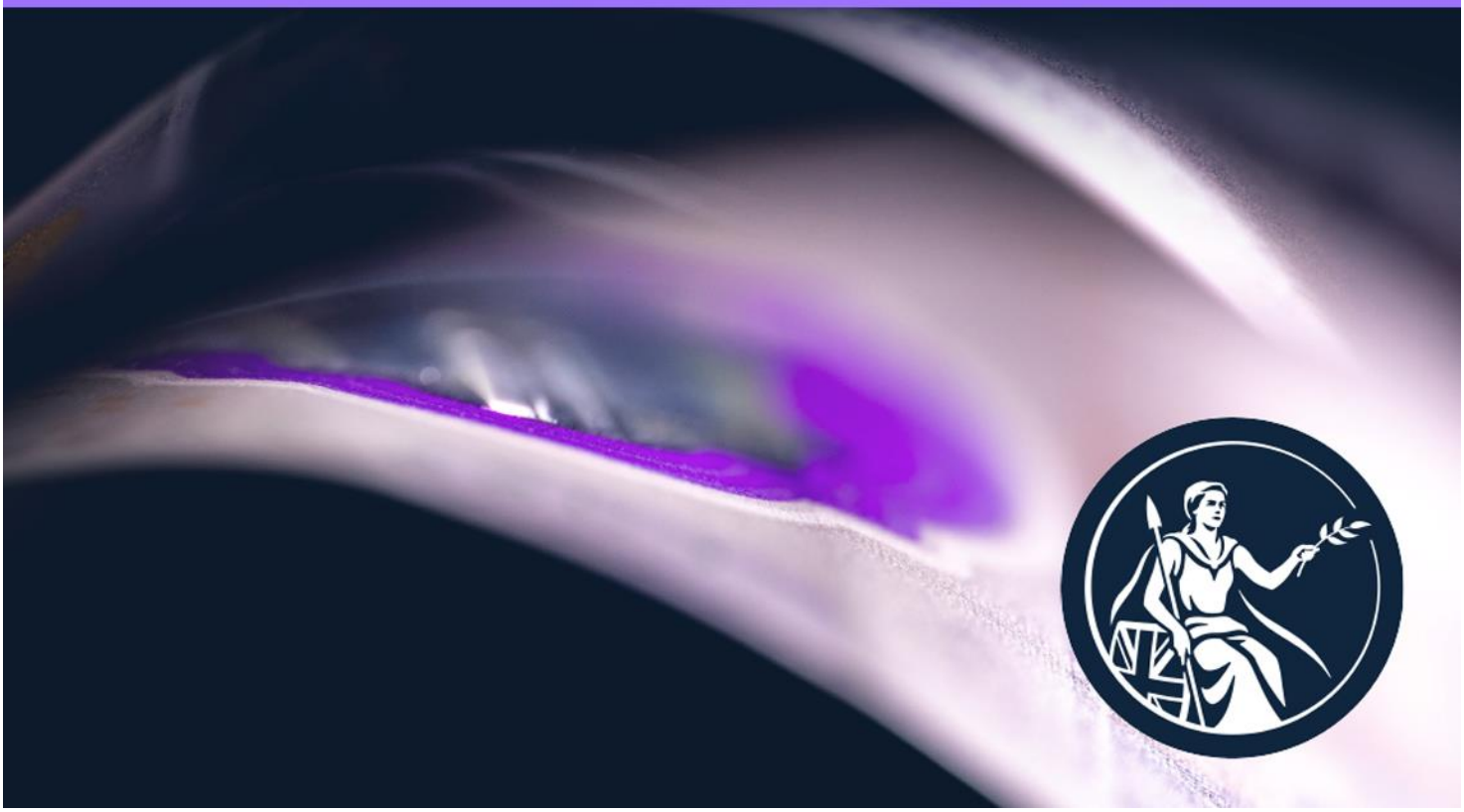
Bank of England PRA

FCA FINANCIAL CONDUCT AUTHORITY

Operational resilience: Critical third parties to the UK financial sector

Supervisory statement | SS6/24

November 2024



Operational resilience: Critical third parties to the UK financial sector

Supervisory statement | SS6/24

November 2024

Prudential Regulation Authority | 20 Moorgate | London EC2R 6DA

Financial Conduct Authority | 12 Endeavour Square | 12 Endeavour Square | London E20 1JN

Bank of England | Threadneedle Street | London EC2R 8AH

Contents

1: Introduction

1.1 This supervisory statement (SS) is issued jointly by the Prudential Regulation Authority (PRA), the Financial Conduct Authority (FCA), and the Bank of England (the Bank) (collectively 'the regulators').

Overall objective

1.2 This SS sets out the regulators' expectations of how a critical third party (CTP) should comply with the duties and obligations placed on it by or under the Financial Services and Markets Act 2000 (FSMA) as amended by the Financial Services and Markets Act 2023 (FSMA 2023), including the requirements in the regulators' rules (collectively referred to as the 'CTP duties').

1.3 The overall objective of the oversight regime for CTPs is to manage risks to the stability of, or confidence in, the UK financial system that may arise due to a failure in, or disruption to, the services (either individually or, where more than one service is provided, taken together) that a CTP provides to 'firms' (as defined in section 2) ('**Overall Objective'**). A CTP should interpret the CTP duties and the accompanying expectations in this SS in light of the Overall Objective.

Format of the regulators' rules for CTPs

1.4 Each regulator has a standalone statutory rulemaking power over CTPs. However, the regulators have a statutory duty to co-ordinate the exercise of their functions over CTPs (s312U of FSMA), including when making rules for CTPs. As a result, the requirements for CTPs are set out in three separate but substantively identical rule instruments.[1]

1.5 While the regulators have different statutory objectives, all three rule instruments impose identical obligations on CTPs and should be interpreted accordingly. Any differences between the instruments stem from non-substantive differences in the regulators' drafting style, and the format of their respective handbooks and rulebooks.

[1] The Bank's rules include a rule intended to provide relief to a CTP in an emergency circumstance when it would be impossible for the CTP and related persons to comply with the Bank's rules. The relevant draft rules are located in the Critical third parties Emergency Provisions Part of the Bank's rules (technically speaking, this is considered a separate, fourth rule instrument). The PRA and FCA do not need emergency rules because the equivalent existing rules in the General Provisions part of the PRA rulebook and the **FCA Handbook** apply to a 'person' which includes a CTP.

1.6 At the start of each section and, where appropriate, other sections of this SS, the regulators have highlighted where the relevant requirements are located in each of their respective rule instruments. References to 'the regulators' rules' in this SS refer to all three instruments.

Structure of this SS

- Section 2 – sets out the key terms used in this SS.
- Section 3 – explains how a CTP could impact the stability of, or confidence in, the financial system.
- Section 4 – provides an overview of the oversight regime for CTPs.
- Section 5 – sets out how a CTP should comply with the CTP Fundamental Rules (FR).
- Section 6 – sets out how a CTP should comply with the Operational Risk and Resilience Requirements.
- Section 7– sets out how a CTP should comply with the requirements on self-assessments, scenario-testing, incident management playbook exercises, and other assurance and information-sharing.
- Section 8 – sets out how a CTP should comply with the requirements on incident reporting, and other notifications.
- Section 9 – sets out how a CTP should comply with the requirements on public references to their designation.
- Section 10 – sets out how a CTP should comply with the requirement to provide the regulators with an address for service in the UK.
- Section 11 – sets out how a CTP should comply with the requirements on record-keeping and emergency relief.
- Section 12 – lists those requirements for a CTP whose implementation is subject to a transitional period starting on the date specified by HM Treasury in the designation order.

Other documents relevant to the CTP oversight regime

1.7 This SS is the main source of guidance for a CTP on how to interpret and comply with CTP duties. In the event of any perceived inconsistencies between the regulators' rules

and this SS, the text of the rules and, if applicable, relevant statutory provisions in FSMA take precedence.

1.8 The regulators have also issued the following documents, which a CTP should refer to as appropriate:

- Guidance on the regulators' use of skilled person reviews on CTPs:
  - Bank/PRA SS7/24 – Reports by skilled persons: Critical third parties;[2] and
  - chapter 12 and 13 of the Critical third parties sourcebook in the FCA Handbook;
- a joint 'Approach to CTP Oversight document', setting out:
  - an overview of the regulators' objectives;
  - how the regulators will identify potential CTPs, and recommend them for designation to HM Treasury (who will make the ultimate decision regarding designation); and
  - how the regulators will oversee CTPs in practice;
- the 'Bank of England's approach to enforcement in respect of critical third parties: statement of policy and procedure'[3] (CTP Enforcement SoP), which is contained in Annex 4 of The Bank of England's approach to enforcement: statements of policy and procedure. The FCA's equivalent and substantively identical approach to enforcement in respect of CTPs can be found in the FCA Handbook: Critical third parties (Statement of Policy) relating to Disciplinary Measures Instrument 2024[4].

1.9 HM Treasury has also laid before Parliament a Memorandum of Understanding, as required by s312V of FSMA, which specifies how the regulators will coordinate the exercise of their respective functions over CTPs.

---

2 November 2024: **www.bankofengland.co.uk/prudential-regulation/publication/2024/november/reports-by-skilled-persons-critical-third-parties-supervisory-statement**.

3 November 2024: **https://www.bankofengland.co.uk/paper/2024/policy-statement/the-bank-of-englands-approach-to-enforcement-changes-to-sop-and-procedure-following-the-fsma-2023**.

4 November 2024: **https://www.handbook.fca.org.uk/instrument/2024/FCA_2024_40.pdf**.

2: Key terms

2.1 The regulators consider it important to define key terms to ensure a clear and consistent understanding by a CTP of the requirements in the regulators' rules, and the accompanying expectations in this SS. This section should be read alongside the relevant definitions in FSMA and the regulators' rules.

Key entities and persons

(1) A **critical third party (CTP)** means an entity designated by HM Treasury in regulations made under s312L(1) FSMA. HM Treasury may designate an entity as a CTP only if it is satisfied that a failure in, or disruption to, services it provides to firms could threaten the stability of, or confidence in, the UK financial system.

(2) **Firms** comprise:

(i) persons authorised by the PRA and/or the FCA (both on a dual-regulated and FCA-solo regulated basis, including UK authorised branches of non-UK firms) (see section 31 of FSMA);

(ii) financial market infrastructure entities (FMI), as defined in s312L(8) of FSMA, including:

- recognised clearing houses, including central clearing counterparties;
- recognised central securities depositories;
- UK recognised investment exchanges;
- recognised payment systems; and
- specified service providers to a recognised payment system.

(iii) relevant service providers, as defined in s312L(8) of FSMA, including:

- authorised payment institutions, small payment institutions or registered account information services providers, as defined by regulation 2(1) of the Payment Services Regulations 2017; and
- electronic money institutions, as defined in regulation 2(1) of the Electronic Money Regulations 2011.

(3) An **employee** is an individual:

(i) who is employed or appointed by a person in connection with its business, whether under a contract of service or for service or otherwise; or

(ii) whose services, under an arrangement between that person and a third party, are placed at the disposal and under the control of that person. The term 'employee' may cover temporary staff and inward secondees to a CTP.

(4) A CTP's **supply chain** is the network of persons or entities that provide infrastructure, goods, services or other inputs directly or indirectly used by a CTP to deliver, support, and maintain a systemic third party service.

(5) A **Key Nth Party Provider** means a person that is part of a critical third party's supply chain and is essential to the delivery of a systemic third party service to one or more firms.

(6) A **Person Connected with a CTP** is defined in s312P(10) of FSMA, and may include:

(i) members of a CTP's group;

(ii) the controller(s) of a CTP ie a person who holds influence over a CTP directly or indirectly through ownership rights (see s422 of FSMA); or

(iii) legal and natural persons mentioned in Part 1 of Sch.15 of FSMA eg an officer or manager of a CTP's parent undertaking. The term 'Person Connected with a CTP' includes persons who came under the definition in s312P(10) of FSMA at any time from the date when the CTP was designated by HM Treasury, but subsequently ceased to do so.

(7) A **Collective Incident Response Framework** means any group involving firms, the regulators or a combination thereof, whose purpose is to facilitate a collective response to incidents that may adversely affect the UK's financial sector, or parts of it.

(8) A **skilled person** is a person appointed to:

(i) make and deliver to the regulators a report under s166 FSMA (as applied by s312 FSMA); or

(ii) collect or update information as required by the regulators under s166A of FSMA (as applied by s312P of FSMA).

Key concepts

(1) **Operational resilience** (in this SS) refers to the ability of firms, their groups, CTPs and the financial sector as a whole to prevent, adapt to, respond to, recover from, and learn from operational disruptions.

(2) **Operational risk** refers to the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (excluding financial events, such as credit losses etc.).[5]

5 See Basel Committee on Banking Supervision's (BCBS) 2021 'Revisions to the principles for the sound management of operational risk' (PSMOR) March 2021, available at **www.bis.org/bcbs/publ/d515.htm**.

(3) **Important business service** includes the definitions in all three regulators' respective rules on operational resilience for firms.[6]

(4) The terms **risk to the stability of, or confidence in, the UK financial system** and **systemic risk** are used interchangeably in this SS and should be interpreted as synonymous.

(5) An **oversight function** refers to a function conferred by FSMA on a regulator in relation to CTPs, including the regulator's statutory powers to:

(i) make rules imposing duties on a CTP in connection with the provision of services to firms (rulemaking powers) (s312M of FSMA) and to oversee compliance with these rules;

(ii) direct a CTP in writing to:

- do anything; or
- refrain from doing anything specified in the direction (s312N-312O of FSMA) (powers of direction and procedure);

(iii) gather information from a CTP and Persons Connected to a CTP, and carry out investigations (s312P of FSMA) (information-gathering and investigations powers);

(iv) take enforcement action against a CTP in certain circumstances (s312Q and s312R of FSMA) (disciplinary and censure powers).

(6) The **regulators' rules** are the separate but substantively identical rule instruments issued by the Bank, FCA and PRA respectively setting out the requirements for CTPs.

(7) **CTP duties** means the duties and obligations placed upon a CTP by or under FSMA, including the regulators' rules.

(8) A **third party arrangement** means any arrangement whereby a person provides a product or service to a firm, whether the product or service:

(i) is one which would otherwise be provided by the firm itself;

(ii) is provided directly or by a sub-contractor; or

(iii) is provided by a person within the same group as the firm eg intra-group services from a parent to its subsidiaries.

(9) A **systemic third party service** means a service (wherever carried out) provided by a CTP to one or more firms, a failure in, or disruption to, the provision of which

6 Rule 1.2 of the **Operational Resilience** part of the PRA Rulebook, **SYSC 15A.2 Operational resilience requirements** and the **Bank of England policy on Operational Resilience of FMIs.**

(either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system.

(10) **An asset** means something, whether tangible or intangible, that is of value, including people, data, information, infrastructure, finances and reputation.

(11) **Disruption** includes (in relation to a systemic third party service):
- (i) a complete or partial failure of that service;
- (ii) a complete or partial degradation to the quality of that service;
- (iii) a complete or partial unavailability of that service; or
- (iv) a service not performing as intended as a whole or in part.

(12) A **CTP operational incident** means either a single event or a series of linked events that:
- (i) causes serious disruption to the delivery of a systemic third party service; or
- (ii) impacts a CTP's operations such that the availability, authenticity, integrity or confidentiality of assets belonging to firms which a CTP has access to as a result of it providing a systemic third party service to those firms is or may be seriously and adversely impacted.

(13) **Affected firm** means, in relation to a CTP operational incident:
- (i) any firm to which a CTP supplies a systemic third party service impacted by that CTP operational incident; or
- (ii) any firm whose assets are or may be seriously and adversely impacted by that CTP operational incident.

(14) **Incident management playbook** is an umbrella term for any document(s) which set out the plans and procedures to be followed by a CTP in the event of a CTP operational incident in order to:
- (i) respond to and recover from the CTP operational incident; and
- (ii) facilitate effective communication with, and support to, the regulators and affected firms (individually and collectively).

(15) **Incident management playbook exercise** means a simulation of a CTP operational incident (based on severe but plausible scenarios) designed to assess the effectiveness of one or more aspects of a CTP's incident management playbook.

(16) The **shared responsibility model** is a model for allocating contractual responsibility between a CTP and its customer firms for aspects of the configuration, deployment or operation of a service including its security and resilience.

(17) Unless otherwise indicated, the following terms in this SS should be interpreted as defined in the **Financial Stability Board (FSB) Cyber Lexicon**:[7]

(i) Authenticity
(ii) Availability
(iii) Confidentiality
(iv) Cyber incident response plans
(v) Cyber Resilience
(vi) Cyber Risk
(vii) Cyber Security
(viii) Insider Threat
(ix) Integrity (except in CTP Fundamental Rule (FR) 1)
(x) Penetration Testing
(xi) Situational Awareness
(xii) Threat Actor
(xiii) Vulnerability (except in section 3 below)

2.2 In this SS:

- 'must' describes a requirement on a CTP imposed by or under FSMA, including the regulators' rules;
- 'should' sets out how the regulators expect a CTP to comply with a requirement. These expectations are outcomes-focused and recognise that there might be a number of ways a requirement can be met;
- when used in the context of the regulators' rules and the accompanying expectations in this SS, 'may' describes a best practice or suggested approach that a CTP can choose to adopt in order to comply with these rules and expectations.

3: How a CTP could impact the stability of, or confidence in, the financial system

How CTPs should use this section

3.1 The Bank's Financial Policy Committee's (FPC) 'Financial Stability in Focus: The FPC's macroprudential approach to operational resilience' [8] illustrates how the resilience of

7 April 2023: **www.fsb.org/2023/04/cyber-lexicon-updated-in-2023**.

8 March 2024: **www.bankofengland.co.uk/financial-stability-in-focus/2024/march-2024**.

individual firms, while providing the essential foundation for operational resilience across the UK financial system, may not, by itself, be sufficient to ensure system-wide resilience. This is due, in particular, to the existence of additional vulnerabilities in the financial system (**macro vulnerabilities**). The oversight regime for CTPs seeks to manage one important source of macro vulnerabilities: the financial system's increasing reliance on certain services that certain third parties ie CTPs provide to firms.

3.2 In light of the Overall Objective, and to clarify and illustrate the potential systemic risk posed by the failure in, or disruption to, a CTP's services to firms, this section applies the analysis in the FPC's macroprudential approach to operational resilience to CTPs.

3.3 To deliver the Overall Objective, it is of vital importance that every CTP clearly understands how disruption to its services to firms (in particular, systemic third party services as defined in section 2), could threaten the stability of, or confidence in, the UK financial system. Every CTP should familiarise itself with this section and apply it to the services it provides to firms. A CTP should develop its understanding of the systemic risks it may pose. This understanding should:

- help a CTP interpret the CTP duties, and comply with their letter and spirit; and
- encourage CTPs to think systemically. The interests of a CTP and its individual customer firms may not always automatically align. It is therefore essential for a CTP to understand how its actions can impact the financial system;
- foster a culture of collaboration between a CTP, firms and the regulators underpinned by the common goal of strengthening the resilience of the financial system.

Limitations on the ability of individual firms to delivery system-wide resilience

3.4 The regulators have introduced requirements and expectations to strengthen the operational resilience of individual firms, and their management of outsourcing and third party risks. Firms and their senior management (including, where applicable, individuals performing Senior Management Functions (SMFs) under the Senior Managers and Certification Regime (SM&CR)) remain accountable for complying with all applicable requirements and expectations. The CTP duties complement, but do not replace, the requirements and expectations placed on firms.

3.5 The requirements and expectations placed on firms seek to manage risks stemming from vulnerabilities in their business models or operational arrangements (**micro vulnerabilities**). However, due to structural features in the financial system, even if

individual firms comply with applicable requirements and expectations (thus strengthening their individual operational resilience), this may not be enough to prevent certain incidents from threatening the stability of, or confidence, in the financial system. These structural features fall under two connected categories: (i) **macro vulnerabilities** and (ii) **transmission channels**, [9] and are central to the FPC's macroprudential approach to operational resilience. They also help explain how a CTP operational incident could threaten the stability of, or confidence in, the UK financial system.

Macro vulnerabilities

3.6 Macro vulnerabilities are inherent in the structure of the financial system, and the collective behaviour of firms and other participants within the system.

3.7 While operational incidents are most likely to originate in a specific part of the financial system, macro vulnerabilities can amplify their impact in ways that can affect financial stability. The FPC's macroprudential approach to operational resilience identifies several macro vulnerabilities, which include:

- concentration;
- interconnectedness;
- correlation and common vulnerabilities;
- complexity and opacity; and
- the financial system's dependence on data. All of these macro vulnerabilities are relevant to the impact that a CTP operational incident could have on the stability of, or confidence in, the UK financial system.

Concentration

3.8 The market for a service is said to be concentrated when customers receiving that service rely on one third party service provider or a small number of third party service providers. Concentration can arise directly as a result of arrangements between multiple firms and a third party service provider, between a systemically important firm and a third party service provider, and/or indirectly through recurrent nth party providers in the supply chains of multiple third party service providers.

3.9 As the FSB's 'Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities' (FSB TPR Toolkit) notes,[10] market concentration in the provision of services to firms does not, by itself, automatically pose systemic risks. In some cases, it can strengthen the operational resilience of firms and, by extension, help promote financial stability.

---

9 In this section, the terms 'micro vulnerability' and 'macro vulnerability' should be interpreted as described in the FPC's macroprudential approach to operational resilience.

10 December 2023: **https://www.fsb.org/wp-content/uploads/P041223-1.pdf**.

3.10 However, concentration is a macro vulnerability because it means that an operational incident at a third party service provider whose services to firms have a high level of market concentration, such as a CTP, can have a disproportionate impact on the financial system. Such a third party service provider can become a single-point-of-failure for the financial system.

3.11 As the FSB TPR Toolkit highlights, the level of market concentration in a single or small number of third parties is a relevant factor to the identification of potential systemic risks, but is not the only factor. Concentration is more likely to lead to systemic risk when it co-exists alongside other factors, which may include the nature of the service(s) provided by that third party service providers, the substitutability of these services, and the systemic significance of the firms that use them.

Interconnectedness

3.12 Firms and other participants in the financial system are highly interconnected, often in complex and opaque ways. These interconnections exist due to, for instance, counterparty relationships. Interconnectedness is a macro vulnerability because it increases the probability that an operational incident originating in one node of the financial system could have a knock-on impact on other nodes, which can in turn impact additional nodes and so on. These knock-on impacts can be facilitated by the transmission channels described below. The complexity and opacity of these interconnections can make it challenging for firms and other participants in the financial system to prevent, adapt to, respond to, recover and learn from operational incidents.

3.13 A CTP is a critical node in the financial system. If it suffers an operational incident, there is a significant risk of knock-on impacts on other nodes in the financial system, which could threaten financial stability. Interconnectedness also means that actions taken by a CTPs or affected firms in response to a CTP operational incident could have unanticipated and unintended consequences in different parts of the financial system, thus threatening its stability.

Common and correlated vulnerabilities

3.14 When micro vulnerabilities are common or correlated across the financial system, they can become a macro vulnerability. This is because when disruption involving such a micro vulnerability occurs, it is likely to affect multiple firms simultaneously. An example might be multiple firms' reliance on the same artificial intelligence/machine learning model (AI) model provided by a CTP leading to herding or procyclical market behaviour. If the model begins not operating as intended (referred to as 'model drift') this could have widespread consequences across the financial system, potentially undermining its

stability.[11] As with interconnectedness, complexity and opacity can amplify the risks posed by correlation and common vulnerabilities.

System-wide dependence on data

3.15 A further macro vulnerability can arise because timely access to accurate data is critical to the functioning of the financial system. A third party service provider, such as a CTP, may have direct access to data belonging to firms that supports their delivery of important business services (IBSs) or is otherwise confidential or sensitive. A breach to that third party service provider's operations – for instance, in the event of a cyber-attack – could threaten the confidentiality, integrity, authenticity or availability of this firm data. This could in turn disrupt payment flows, impede price discovery or lead to a loss of confidence in the financial system (see below). Difficulty restoring access to this data and gaining reassurance about its authenticity or integrity could also lengthen recovery times following a CTP operational incident. The regulators' definition of a CTP operational incident recognises the financial system's dependence on data. It is important to note, however, that firms can and must take certain actions to manage this risk and mitigate its impact if it crystallises, such as appropriately classifying and encrypting their data.

Transmission channels

3.16 A CTP operational incident could transmit through the financial system through one or more of the transmission channels examined below, thereby amplifying its effect on the macro vulnerabilities discussed above and, by extension, the stability of, or confidence

[11] "Model drift refers to the degradation of machine learning model performance due to changes in data or in the relationships between input and output variables. Model drift—also known as model decay—can negatively impact model performance, resulting in faulty decision-making and bad predictions." (**What Is Model Drift? | IBM**)

in, the UK financial system.

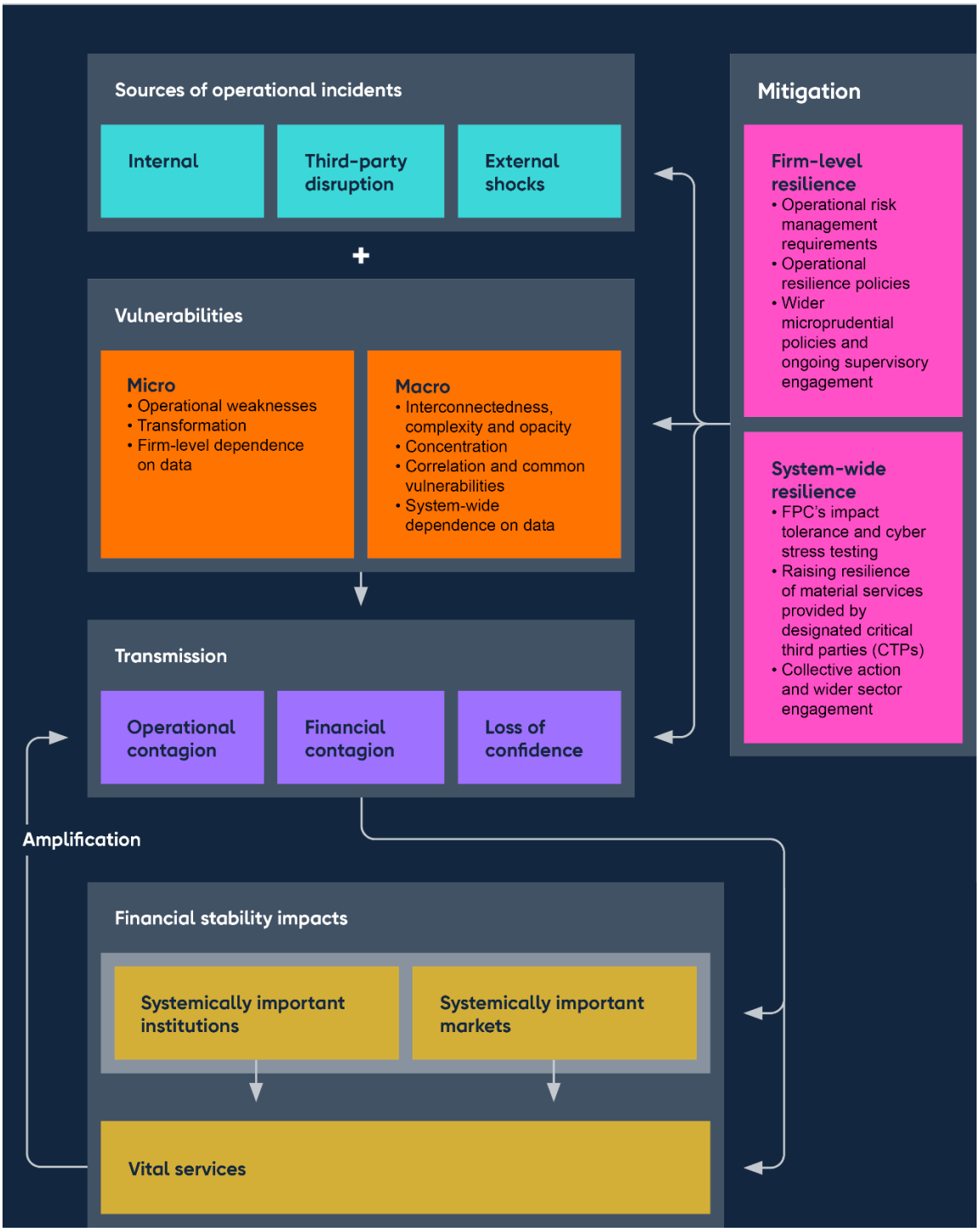


Figure 1: The FPC's approach to assessing financial stability risks from potential operational incidents[12]

12 www.bankofengland.co.uk/financial-stability-in-focus/2024/march-2024

Contagion

3.17 Contagion occurs when an operational incident causes further disruption elsewhere in the financial system or the real economy. This can occur via operational or financial impacts:

- Operational contagion occurs when an initial operational disruption causes further operational disruption elsewhere. A CTP operational incident that seriously affected the IBSs of its customer firms could leave them unable to transact with other firms or participate in financial markets. This could have knock-on impacts on those firms' counterparties, who may, as a result, be unable to undertake their own activities. If operational contagion is extensive, market-wide disruption could occur.

- Financial contagion occurs when operational disruption has financial impacts that cause further disruption. For instance, a CTP operational incident could result in financial contagion if it affected liquidity flows among firms. If firms that depend on a CTP's services to send payments became unable to do so as a result of a CTP operational incident, this could cause liquidity shortages at other firms who rely on incoming payments from these firms to fund their outgoing payments as part of their intraday liquidity management.

Loss of confidence

3.18 The effects of an operational incident can also spread through the financial system via a loss of confidence. As noted in the FPC's macroprudential approach to operational resilience, while operational and financial contagion can be potentially mitigated with workarounds (such as manual processing where automated systems are impaired, or alternative sources of funding), confidence can be difficult to restore once lost. For this reason, a loss of confidence in the financial system, or parts thereof, is the transmission channel by which an operational disruption (including as a result of a CTP operational incident) could most likely lead to financial instability.

3.19 A CTP operational incident could cause the customers or counterparties of affected firms to lose confidence in these institutions or the CTP where the incident originated. Moreover, if firms not directly affected by the original CTP operational incident are subsequently perceived to be vulnerable to the same or similar incidents, a more widespread loss of confidence could result. This could in turn trigger panicked reactions, such as bank runs, or disruption to liquidity flows if firms become reluctant to extend credit or liquidity. If the loss of confidence is pervasive and significant, or if it affects one or more systemically important firms, it could threaten financial stability. Adverse coverage of a CTP operational incident in mainstream and social media could accelerate

and amplify the risk of a loss of confidence in the financial system, including through the dissemination of disinformation and misinformation about the incident and its impact.

3.20 The importance of a loss of confidence as a transmission channel is explicitly reflected in the statutory test for designation as a CTP (s312L(2) of FSMA).

Interaction of macro vulnerabilities and transmission channels

3.21 A CTP operational incident that led to systemic risk could involve the interaction of several macro vulnerabilities and transmission channels. For instance, the incident could begin with disruption to one or more of a CTP's systemic third party services impacting a large number of the CTP's customer firms due to concentration. The impact of the incident could then spread to other parts of the financial system through financial and/or operational contagion as a result of the interconnections of those affected firms with other firms and market participants. This could in turn trigger a loss of confidence in those firms, parts of the financial system or the financial system as a whole. The end result could be a threat to financial stability.

4: Overview of the oversight regime for CTPs

The role of the CTP regime in building system-wide resilience

4.1 The CTP oversight regime seeks to build system-wide operational resilience. It sits alongside, and complements, the requirements and expectations for firms relating to operational resilience, outsourcing and third party risk management.

4.2 A CTP's compliance with the CTP duties should lead to progressive improvements to the resilience of its systemic third party services, thus mitigating the potential systemic risks posed by a CTP by reducing the:

- likelihood and frequency of CTP operational incidents; and
- the impact of these incidents when they do occur (like the operational resilience regime for firms, the CTP oversight regime assumes that CTP operational incidents are inevitable).

Focus on CTPs' services to firms

4.3 Although HM Treasury designates a CTP at the entity level, the oversight regime for CTPs only applies in relation to the services that a CTP provides to firms. The term service should be interpreted broadly in light of the Overall Objective. It includes, but is not limited to:

- a facility, as noted in s312L(8) of FSMA;
- activities, functions, processes and tasks, as noted in the FSB TPR toolkit;[13] and
- Information and Communications Technology (ICT) Services.

Systemic third party services

4.4 The regulators' statutory powers extend to all the services that a CTP provides to firms. However, most of the regulators' rules that impose significant obligations on a CTP apply only in relation to its provision of systemic third party services to firms (except CTP Fundamental Rule (FR) 6 (see section 5).

4.5 Section 3 of the regulators' joint 'Approach to CTP Oversight' (CTP Approach Document) explains how systemic third party services will be identified during the process leading to the designation of a third party service provider as a CTP by HM Treasury, and reviewed regularly thereafter. The document outlines that regulators will periodically review whether a CTP continues to meet the criteria for designation and update HMT accordingly. The

13 **www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities**.

regulators will also consider and flag if there have been changes to the systemic third party services, (i.e. due to significant changes in the way they are provided, technology developments etc). CTPs will be informed of the regulators review and outcome.

4.6 The phrase 'wherever carried out' in the definition of a systemic third party service clarifies that, as long as the systemic third party service is provided to one or more UK firms, it is in scope of the regulators' rules irrespective of the jurisdiction(s) from which it is provided. This is an important clarification, as a CTP may provide a systemic third party service to firms from one or more jurisdictions outside the UK, including where it relies on its global supply chain to deliver this service or parts thereof.

4.7 The phrase 'either individually or, where more than one service is provided, taken together' clarifies that a systemic third party service can comprise a single service, or a group of connected services taken together. A group of connected services many be treated as a single systemic third party service if these services are connected in such a way that the disruption or failure of one service could cause the disruption or failure of one, more or all of the services to which it is connected.

4.8 Consistent with the Overall Objective, a CTP should treat anything that could reasonably affect the resilience of a systemic third party service as being in scope of the regulators' rules. For instance, the resources used to deliver, maintain and support that service as identified in a CTP's mapping (see section 6).

4.9 In addition to a CTP operational incident, the resilience of a systemic third party service could be affected by developments including but not limited to significant changes to:

- the CTP's:
  - board, senior management or organisational structure;
  - financial or operational resilience;
  - controls, policies and procedures;
  - way of providing one or more systemic third party services; or
- legal or regulatory developments in the UK or any other jurisdiction.

Non-systemic third party services

4.10 While the regulators' rules apply, for the most part, to the systemic third party services a CTP provides to firms, a CTP should ensure that all its services to firms meet appropriate levels of resilience that reflect their importance and the risks they pose. The CTP Approach Document provides non-exhaustive examples of circumstances where the regulators may look at a CTP's non-systemic third party services or their oversight.

4.11 A CTP may choose to voluntarily apply certain requirements in the regulators' rules, such as the Operational Risk and Resilience Requirements in section 6, and the relevant

accompanying expectations in this SS to some or all its non-systemic third party services as best practice.

No requirement to establish a UK subsidiary or branch

4.12 There is no requirement for a CTP whose head office is outside the UK (and which did not already have a UK subsidiary or branch prior to being designated as a CTP by HM Treasury) to establish a UK subsidiary or branch under the CTP oversight regime. This is because, as explained above, the CTP oversight regime applies to a CTP's services to firms regardless of where they are provided from. In addition, certain requirements in the regulators' rules seek to ensure that every CTP:

- appoints a central point of contact for the regulators (see section 5); and
- provides the regulators with a UK address for service for documents, including 'relevant documents' eg statutory notices issued under FSMA (see section 10).

CTPs that are part of a group

4.13 The regulators' rules apply to and are enforceable against the entity or entities listed in the HM Treasury regulations designating a CTP. However, that entity or entities may rely on other undertakings in its or their group [14] for the delivery of systemic third party services to firms, or other aspects relevant to its or their compliance with the CTP duties. Where this is the case:

- the regulators' information-gathering powers in S312P of FSMA extend to 'Persons Connected to a CTP', which include undertakings in the CTP's group. The regulators can therefore request information directly from these undertakings;
- under Requirement 3: Dependency and supply chain risk management, a CTP must take reasonable steps to ensure that all undertakings in its group that are part of its supply chain cooperate with it in meeting the CTP duties (see section 6); and
- CTP FRs 2, 3 and 5 implicitly require a CTP to ensure that others in its group facilitate its compliance with the CTP duties.

4.14 As part of its obligations under CTP FR6, a CTP should inform the regulators of any changes to its group structure that may:

- prompt a reconsideration as to the appropriate entity or entities that should be listed in HM Treasury's designation regulations; and/or
- impact its delivery of systemic third party services to firms.

14 As defined in s421 of FSMA.

Interaction with the requirements for firms

4.15 As noted in section 3, the CTP duties complement the requirements and expectations for firms on operational resilience, outsourcing and third party risk management. 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 (including individuals performing SMFs).

4.16 For instance, as noted in PRASS2/21–Outsourcing and third party risk management,[15] the Bank's FMI outsourcing and third party risk management policy statement;[16] SYSC 8 in the FCA Handbook[17] and the FSB TPR toolkit, firms should 'determine the materiality of every outsourcing and third party arrangement and perform appropriate and proportionate due diligence on all potential service providers', regardless of whether they are CTPs or not.

4.17 The CTP oversight regime does not impose additional requirements on firms in relation to operational resilience, and outsourcing and third party risk management, although it references these requirements where relevant.

The shared responsibility model and its limitations

4.18 Some arrangements between CTPs and firms may be contractually governed by the shared responsibility model (defined in section 2). A CTP's duties under the oversight regime should generally align to its areas of responsibility under the shared responsibility model. CTPs are not required or expected to assume responsibilities that clearly fall to their customer firms. Moreover, during a CTP Operational Incident, it is likely that both CTPs and affected firms will need to take a combination of individual and collective response and recovery measures in line with their respective regulatory obligations.

4.19 While the shared responsibility model is relevant to the demarcation of the CTP duties, the model is not designed with systemic risk in mind. The shared responsibility model sets out the respective responsibilities of two parties to a transaction (the CTP and the firm) but, in doing so, does not consider the cumulative impact of the disruption or failure of the services that the CTP provides to multiple firms (which may in turn be interconnected with one another and other parts of the financial system, as explained in section 3). The fact that the shared responsibility model does not recognise the asymmetric impact of a CTP not meeting its responsibilities, relative to the impact of an individual customer firm not

15 March 2021: **https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf**.
16 February 2023: **https://www.bankofengland.co.uk/paper/2023/ps/fmi-outsourcing-third-party-risk-management-ps**.
17 **https://www.handbook.fca.org.uk/handbook/SYSC/8/1.html**.

doing so limits its applicability as a tool to manage systemic risk. The CTP duties and the accompanying expectations in this SS seek to address the inherent gap in the shared responsibility model when it comes to managing systemic risk.

Alignment to international standards and interoperability with similar non-UK regimes

4.20 Alignment with relevant international standards, in a manner which accounts effectively for UK circumstances, promotes trust and confidence among key stakeholders in the UK regulatory framework, and provides stability and predictability for firms that operate across multiple jurisdictions. This helps to support the UK's position as a global financial centre, and its international competitiveness and growth over the medium to long term. The oversight regime for CTPs draws inspiration from and seeks to be consistent with global standards and guidance. In particular:

- the FSB:
  - Cyber Lexicon;
  - FSB TPR toolkit;
  - Effective Practices for Cyber Incident Response and Recovery;[18] and
  - Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report.[19]

- the Basel Committee on Banking Supervision (BCBS):
  - Principles for Operational Resilience;[20] and
  - Revised Principles for the Sound Management of Operational Risk (PSMORs).

- the Committee on Payments and Market Infrastructures-International Organization of Securities Commissions (CPMI-IOSCO):
  - Principles for financial market infrastructures (PFMIs) in particular, the 'Oversight expectations applicable to critical service providers' (Annex F);[21] and
  - PFMIs: Assessment methodology for the oversight expectations applicable to critical service providers.[22]

- the G7 Cyber Expert Group: Fundamental Elements series.[23]

18 October 2020: **https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/**

19 April 2023: **https://www.fsb.org/2023/04/recommendations-to-achieve-greater-convergence-in-cyber-incident-reporting-final-report/**.

20 March 2021: **https://www.bis.org/bcbs/publ/d516.htm**.

21 April 2012: **https://www.bis.org/cpmi/info_pfmi.htm**.

22 December 2014: **https://www.bis.org/cpmi/publ/d123.htm**

23 February 2023: **https://www.gov.uk/government/collections/g7-cyber-expert-group-fundamental-elements-series**.

4.21 The UK oversight regime for CTPs is designed to be interoperable with similar non-UK regimes, such as the Digital Operational Resilience Act (DORA) in the European Union (EU), and the Bank Service Company Act in the United States but only to the extent that such interoperability does not conflict with or undermine the Overall Objective.

4.22 The CTP approach document sets out some ways in which the regulators may coordinate with (i) non-UK financial regulatory and supervisory authorities in, and (ii) relevant UK non-financial authorities in their oversight of CTPs.

Proportionality

4.23 All CTPs are subject to common, minimum requirements, expectations and oversight that reflect the potential systemic risk they pose. However, the regulators will take a proportionate approach to the application of their rules, the expectations in this SS and the exercise of their oversight functions. In so doing, to ensure the regime is not unduly burdensome, the regulators will be guided by the Overall Objective and adapt their approach depending on the specific circumstances of a CTP.

4.24 In considering the application of proportionality to different CTPs, the regulators may have regard to matters such as:

- the number, nature and scale of systemic third party services it provides to firms;
- the potential risks of the failure or disruption of the CTP's systemic third party services to the stability of, or confidence in, the UK financial system;
- the responsibilities of firms under the UK regulatory system, including but not limited to in relation to operational resilience, operational risk and outsourcing and third party risk management.

4.25 If a CTP provides services to multiple sectors and/or jurisdictions, it may be able to use its existing processes and systems in relevant areas e.g. risk management, technology and cyber resilience etc to try to demonstrate to the regulators that it is meeting the Overall Objective and complying with the regulators' rules, and the accompanying expectations in this SS. However, it will be for the regulators to ultimately assess whether these processes are sufficient

5: CTP Fundamental Rules

5.1 This section sets out how a CTP should comply with the CTP Fundamental Rules in the:

- Critical third parties Fundamental Rules (chapter 3) in the Critical third parties Part of the PRA Rulebook, and Bank of England FMI Rulebook;[24] and
- chapter 3 of the Critical third parties sourcebook in the FCA Handbook.

Box 1: CTP Fundamental Rules

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

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

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

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

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

CTP Fundamental Rule 6: A CTP must deal with each regulator in an open and cooperative way, and must disclose to each regulator appropriately anything relating to the CTP of which it would reasonably expect notice.

Scope of application

5.2 The CTP Fundamental Rules are high level rules that collectively act as an expression of the Overall Objective and provide a general statement of a CTP's fundamental obligations under the oversight regime.

5.3 CTP Fundamental Rules 1-5 apply only in relation to a CTP's provision of systemic third party services to firms. CTP Fundamental Rule 6 applies in relation to all the services that a CTP provides to firms.

[24] The Bank of England FMI Rulebook will be published in 2025. In the interim, these rules can be accessed on the Bank's website.

5.4 The rationale for applying CTP Fundamental Rule 6 in relation to all the services a CTP provides to firms is to ensure that the regulators receive all information from a CTP that might be relevant to their oversight functions. Without this information, the regulators may not be able oversee CTPs effectively, including taking any necessary steps to mitigate current or future risks.

How a CTP should interpret the CTP Fundamental Rules

5.5 A CTP should interpret the CTP Fundamental Rules consistently with the Overall Objective. This includes terms used in these rules such as ‘effective’, ‘integrity’, ‘prudent’, ‘responsibly’ etc.

CTP Fundamental Rule 3

5.6 For instance, acting “in a prudent manner” under CTP Fundamental Rule 3 includes a CTP acting in a way that ensures that:

- its culture and processes support the Overall Objective;
- it has adequate resources, including financial, human and technology resources to support its provision of systemic third party services to firms in times of business as usual, financial distress and during a CTP Operational Incident; and
- it takes reasonable steps to ensure that its infrastructure, and that of its Key Nth Party Providers, are resilient.

CTP Fundamental Rule 6

5.7 Likewise, the requirement to “disclose to the Regulator appropriately anything relating to the CTP of which they would reasonably expect notice” under CTP Fundamental Rule 6 should be interpreted as encompassing any information relevant to the CTP duties or the Overall Objective.

5.8 Below is a non-exhaustive list of matters which the regulators would reasonably expect a CTP to provide notice of under CTP Fundamental Rule 6:

- significant changes to the CTP’s business that are relevant to the Overall Objective or the CTP duties, including to its:
    - corporate or group structure eg the acquisition of a company that will be essential to the provision of services to firms;
    - governing body (board of directors), senior management or, if different, the top layer of decision-makers responsible for the delivery of services to firms;
- changes to the systemic third party services it provides to firms, including:

- changes to the risk profile of these services;
- changes to the appropriate maximum tolerable level of disruption of these services (see Section 6);
- planned major change management programmes affecting these services;
- the planned or unplanned discontinuation or termination of these services;
- changes to the resources essential to the delivery of these services, including key Nth party providers; or
- the transfer of responsibility for the delivery of these services (or key parts thereof) to a Person Connected to a CTP or a key Nth party provider; or
- changes to the geographical location(s) ie jurisdictions from which a CTP provides or can provide these services, including back-up locations.

- advance warning of incidents that may not (at the time of providing notice to the regulators) come under the definition of a CTP Operational Incident (and are therefore not subject to the incident reporting requirements in the regulators' rules) but are highly likely to meet that definition imminently or in the short-term;
- advance warning of relevant legal or regulatory changes in the UK or any other jurisdiction; and
- any matter which could:
  - have a significant adverse impact on a CTP's reputation; or
  - affect a CTP's ability to supply systemic services to firms or to comply with its CTP duties.

5.9 While the CTP Fundamental Rules do not include an explicit requirement on CTPs to be open and co-operative with the firms they provide systemic third party services to, the regulators' rules include several requirements for CTPs to share information with these firms, including a requirement for CTPs to "have in place effective and secure processes and procedures to ensure sufficient and timely information is given to a firm to which it provides any systemic third party services to enable that firm to manage adequately risks related to its use of the CTP's systemic third party services" (see section 7). A CTP should comply with all these requirements in an open and cooperative way, and in line with the spirit as well as the letter of the relevant rules. This may involve a CTP sharing information with firms beyond that explicitly required by the regulators' rules if appropriate.

6: Operational Risk and Resilience Requirements

6.1 This section sets out how a CTP should comply with the Operational Risk and Resilience Requirements in:

- the 'CTP Operational Risk and Resilience Requirements' (chapter 4) in the Critical third parties Parts of the PRA Rulebook, and Bank of England FMI Rulebook; and
- chapter 4 of the Critical third parties sourcebook in the FCA Handbook.

6.2 A CTP must have in place sound, effective and comprehensive strategies, controls, processes, and systems that enable it to comply with the regulators' rules.

6.3 The CTP Operational Risk and Resilience Requirements only apply in relation to the provision of a CTP's systemic third party services to firms.

6.4 As part of its compliance with the Operational Risk and Resilience Requirements, and to achieve the Overall Objective, a CTP should seek to continuously improve the resilience of its systemic third party services as it learns from incidents, exercises and testing (including but not limited to those required by the regulators' rules (see section 7)).

Requirement 1: Governance

A CTP must ensure that its governance arrangements promote the resilience of any systemic third party service it provides, including by:

(1) appointing one or more individuals who:

(a) are employees of the CTP or members of its governing body; and

(b) possess the appropriate authority, knowledge, skills and experience,

to act as the central point of contact with the regulators in their capacity as authorities having oversight functions;

(2) establishing clear roles and responsibilities at all levels for its staff who are essential to the delivery of a systemic third party service, with clear and well-understood channels for communicating and escalating issues and risks;

(3) establishing, overseeing and implementing an approach that covers the CTP's ability to prevent, respond and adapt to, as well as recover from, any CTP operational incident

(4) implementing lessons learnt from CTP operational incidents and any testing and exercising undertaken, including but not limited to that undertaken in accordance with 5;

(5) ensuring appropriate review and approval of any information provided to the regulators;

(6) notifying the *regulators* in writing of:

(a) the names of the individuals appointed under (1);

(b) the business address of those individuals; and

(c) the email address, telephone number and out of hours contact details for each of those individuals; and

(7) notifying the *regulators* of any changes to the information notified under (6) as soon as is practicable.

Appointment of a central point of contact for the regulators

6.5 Regardless of whether a CTP appoints an individual or a team as the central point of contact for the regulators, it should ensure that the responsibilities of the individual or team members are clearly allocated and documented (especially if they are shared or split among more than one individual), and that the individual or team have up to date knowledge, skills and experience of:

- the CTP's operations and the services that it provides to firms. In particular, systemic third party services;

- the Overall Objective, CTP duties and the accompanying expectations in this SS; and

- any requirements and expectations applicable to the firms that the CTP provides services to that are relevant to its provision of services to these firms, in particular, those relating to operational resilience, outsourcing and third party risk management.

6.6 The central point of contact's knowledge of financial regulation should be sufficient to enable a CTP to comply with the CTP duties. A CTP should implement appropriate training to develop and update knowledge of relevant financial regulation among individuals at the central point of contact and, to the extent appropriate, other employees essential to the delivery of systemic third party services to firms.

6.7 Requirement 1 also imposes an obligation on the CTP to notify the regulators in writing of:

- the names of any individual(s) appointed to act as the central point of contact with the regulators;
- the business address of those individuals;
- the email addresses, telephone numbers and out of hours contact details for each of those individuals; and
- any changes to the information notified under the previous three bullets as soon as practicable.

6.8 The individual(s) appointed as the designated point of contact should be contactable:

- during UK business hours; and
- outside of UK business hours as required during a CTP operational incident, regardless of whether they are located in the UK or not.

6.9 Where requested to do so by the regulators, the designated point of contact should:

- facilitate the regulators' engagement with other employees of the CTP, such as subject matter experts or individuals responsible for taking decisions relating to the delivery of systemic third party services to firms; and
- engage on the regulators' behalf with undertakings in the CTP's group not designated as CTPs, but which support its delivery of systemic third party services to firms, or its compliance with the CTP duties.

Appropriate review and approval of information provided to the regulators

6.10 A CTP must ensure that any information it provides to the regulators undergoes appropriate review and approval. What constitutes appropriate review and approval will vary depending on a CTP's organisational structure; and on the importance, nature, and time-sensitivity of the relevant information. Documents such as a CTP's self-assessments

should be approved and reviewed by the top layer of decision-makers responsible for the delivery of systemic third party services to firms (see section 7). This layer could be the CTP's governing body or a committee thereof; its senior management; or a specialist committee, individual, or group.

Requirement 2: Risk management

A CTP must manage effectively risks to its ability to deliver a systemic third party service including by:

(1) identifying and monitoring relevant external and internal risks;

(2) ensuring that it has in place risk management processes that are effective at managing those risks; and

(3) regularly updating its risk management processes to reflect issues arising and lessons learned from:

(a) CTP operational incidents;

(b) engagement with the regulators;

(c) new and emerging risks; and

(d) any associated testing and exercising, including but not limited to that carried out in accordance with Requirement 5.

6.11 Many of the risks to a CTP's delivery of systemic third party services are likely to be operational risks. Examples include, but are not necessarily limited to:

- dependency and supply chain risks (see Requirement 3);
- cyber and technology risks (see Requirement 4);
- data risks;
- insider risks eg from current and former employees; and
- risks to the CTP's physical assets eg from fire and natural disasters, or to its energy supply.

6.12 There are two specific risks that are considered individually in Requirements 3 and 4 given their importance and relevance to the CTP oversight regime namely (i) dependency and supply chain risks, and (ii) cyber and technology risks. A CTP must manage all risks, including those covered in Requirements 3 and 4, as part of its risk management processes under Requirement 2 and avoid unnecessary silos.

6.13 A CTP should also consider financial risks that may affect its ability to deliver systemic third party services or meet the CTP duties. In particular, risks to its financial viability. Although the regulators' rules do not impose detailed prudential requirements on CTPs akin to those imposed on firms (eg capital, leverage, liquidity), a CTP should consider how financial risks could impact its provision of systemic third party services, and have in place appropriate transitional measures to respond to the unexpected termination of these services, including due to insolvency (see Requirement 8). A CTP should be able to provide evidence of its ongoing financial viability and its financial risk management to the regulators upon request. In some instances, this evidence might be publicly available, such as where a CTP is publicly listed or belongs to a publicly listed undertaking or group.

Requirement 3: Dependency and supply chain risk management

A CTP must (as part of its obligation under Requirement 2) identify and manage any risks to its supply chain that could affect its ability to deliver a systemic third party service.

A CTP must take reasonable steps to ensure that its Key Nth party providers and persons connected with a CTP that are part of its supply chain:

(1) are informed of the CTP duties that apply to the CTP;

(2) cooperate with the CTP in meeting those CTP duties; and

(3) provide the regulators with access to any information relevant to the exercise of their oversight functions.

6.14 In line with the principle of proportionality and the FSB TPR toolkit, when managing dependency and supply chain risks, a CTP should focus primarily on its Key Nth party providers (as defined in section 2), as they make up the parts of its supply chain that are essential to the delivery of systemic third party services.

6.15 It is possible for the same entity (eg an undertaking in the CTP's group) to be both a Person Connected with the CTP, and a Key Nth Party Provider to that CTP.

6.16 With respect to its Key Nth party providers, a CTP should:

- perform appropriate due diligence before entering into, or significantly changing, contractual arrangements that are key to its delivery of systemic third party services, and monitor these arrangements on an ongoing or regular (at least annual) basis thereafter;

- be transparent with the regulators (in line with CTP FR 6) and the firms it provides systemic third party services to about which parts of its supply chain are essential to its delivery of systemic third party services. CTPs may leverage other regulatory regimes' requirements to obtain this information and provide it to the regulators and to relevant firms;

- where a CTP operational incident is caused by an incident in its supply chain, obtain relevant information about the parts of its supply chain that caused or contributed to the CTP operational incident, and share it with the regulators and affected firms.

- include scenarios involving supply chain disruption in its scenario-testing and incident management playbook exercises. For instance:

    - disruption to a supporting service provided by a Key Nth Party Provider, (see Section 7); or

    - the insolvency of a Key Nth Party Provider; and

- incorporate lessons learned from disruption to its supply chain, and relevant exercises and tests, into its risk management and incident management processes.

6.17 A CTP should review contractual agreements with its Key Nth Party providers entered into prior to its designation at the first appropriate contractual renewal or revision point following its designation, and update them to bring them in line with the CTP duties (see section 12).

6.18 The regulators acknowledge that, when sharing information regarding its supply chain, a CTP may need to consider confidentiality and security issues, such as the protection of personal data and proprietary information of its Key Nth Party providers. When deciding what information to share about its supply chain, a CTP should consider:

- the relevance of this information to the Overall Objective and the CTP duties, including but not limited to CTP Fundamental Rule 6 and Requirement 3; and

- ways to protect any confidential or sensitive information while complying with these duties.

Requirement 4: Technology and cyber resilience

A CTP must (as part of its obligation under Requirement 2) take reasonable steps to ensure the resilience of any technology that delivers, maintains or supports a systemic third party service, including by having:

(1) (as part of its obligation under Requirement 2) sound, effective and comprehensive strategies, processes and systems to adequately manage risks to its technology and cyber resilience; and

(2) regular testing and exercising of those strategies, processes and systems (including as part of its obligations under the regulators' rules (see section 6)) and processes and measures that reflect lessons learned from that testing and exercising.

6.19 Although all Operational Risk and Resilience Requirements are relevant to a CTP's technology and cyber resilience, this area warrants individual consideration due to the:

- importance of technology to the provision of most systemic third party services to firms;
- ever-growing complexity of technology, which can make risks difficult to monitor and manage;
- techniques used by persistent and capable threat actors, which can make it difficult to identify cyber-attacks, contain or fully recover from the damage they cause;
- broad range of entry points through which a CTP can be compromised, including its supply chain (see Requirement 3); and
- potential for cyber-risks to crystalise and propagate rapidly and stealthily.

6.20 Consequently, in addition to complying with the remaining Operational Risk and Resilience Requirements, a CTP's technology and cyber risk management should include:

- processes and measures that identify, assess, mitigate, measure and manage technology and cyber risks. In addition to technology, these processes should cover relevant non-technology elements such as:
    - people, processes and non-technology physical components; and
    - the CTP's supply chain (see Requirement 3);

- measures to protect, detect, respond, and recover critical assets from IT disruptions and cyber-attacks;
- controls that minimise the likelihood as well as the impact of cyber incidents on systemic third party services, including on the resources that deliver, support and maintain these services;
- capabilities to monitor for anomalous activity (in real-time or near-real time) and detect potential cyber incidents;
- capabilities to identify, assess and promptly remediate vulnerabilities relating to information and technology assets;
- threat intelligence, which ensures situational awareness for a CTP to understand the threat environment in which it operates and the adequacy of its cyber risk management;
- processes to assess the impact of cyber incidents, including possible amplification channels and potential systemic risks; and
- response and recovery measures, which should assume the failure of preventative controls.

6.21 A CTP's compliance with recognised standards on cyber security and related areas can provide partial, supporting evidence of its compliance with Requirement 4. For instance, by confirming that the CTP has certain controls in place. However, recognised standards may not always provide all the assurance that the regulators need. For instance, on the effectiveness of these controls. CTPs may therefore need to provide additional assurance that they are complying with Requirement 4 (see section 7).

Requirement 5: Change management

A CTP must ensure that it has a systematic and effective approach to dealing with changes to a systemic third party service, including changes to the processes or technologies used to deliver, maintain or support a systemic third party service, including by:

(1) implementing appropriate policies, procedures and controls to manage effectively the resilience of any change to a systemic third party service;

(2) implementing any change to a systemic third party service in a way that minimises appropriately the risk of any CTP operational incident occurring; and

(3) ensuring that prior to being implemented, any change is appropriately risk-assessed, recorded, tested, verified and approved.

6.22 A CTP's review and approval of changes to its systemic third party services should cover the lifecycle of the relevant changes and consider:

- inherent and residual risks;
- the need for appropriate resources to ensure the resilience and success of the proposed change;
- any new processes that need to be implemented;
- changes to people, including employees, Key Nth party providers and other parts of the supply chain essential to the delivery of the service;
- changes to the risk profile of existing systemic third party services (including risk thresholds or limits);
- the use of appropriate metrics to assess and monitor risks relating to the proposed change;
- the appropriate timeframe for implementation, which should not incentivise undue risk-taking or rushed decision-making;
- the implementation of appropriate controls, risk management and risk mitigation processes; and
- the need for effective and timely communication to customer firms that rely on those services about the proposed changes and their potential impact.

6.23 A CTP may be able to leverage existing and new controls as part of its approach to change management. To minimise the risk of a failure or undue disruption, the regulators expect that before commencing a change to a systemic third party service, a CTP should plan what it will do if the change results in a CTP operational incident. This may include, but is not limited to, reversing or rolling back the change.

6.24 A CTP should continue monitoring changes to systemic third party services for an appropriate period following implementation to identify and manage any unexpected risks.

Requirement 6: Mapping

A CTP must:

(1) within 12 months of being designated by HM Treasury, identify and document:

(a) the resources, including the persons (including key nth-party providers), assets, supporting services and technology, used to deliver, support, and maintain each systemic third party service it provides; and

(b) any internal and external interconnections and interdependencies between the resources identified under (a) in respect of that service; and

(2) thereafter regularly update the process conducted under (1).

6.25 Mapping should enable a CTP to:

- distinguish those resources across the supply chain that are essential to its delivery of systemic third party services, and any interconnections between them;
- inform the design of exercises and tests carried out by a CTP, which, among other objectives, should regularly assess whether these resources are fit-for-purpose (see section 7); and
- identify concentrations and potential single-points-of-failure in its supply chain. For instance, specific Nth party providers, services, geographic regions etc.

6.26 If two or more systemic third party services are supported by the same resources, a CTP may conduct a single mapping exercise for them, but should make clear all the systemic third party services it applies to.

6.27 Although there is no prescribed format or template for a CTP's mapping, it should:

- focus on the resources that are essential to the CTP's delivery of systemic third party services;
- be of a sufficient level of granularity to meet the outcomes in paragraph 6.25; and
- be updated at least annually and following any significant changes to the resources essential to the delivery of the systemic services, including (but not limited to) a change to a key Nth party provider.

6.28 Table 1 provides an illustrative, non-exhaustive list of resources that a CTP's map(s) may include. However, each CTP is responsible for developing its own mapping methodology and identifying the resources essential for delivering, supporting and maintaining its systemic third party services, including any not listed below.

6.29 A CTP's mapping should be proportionate to the nature, scale and complexity of its business. Nevertheless, a CTP's mapping should meet the outcomes described above. A CTP may use additional tools to meet these outcomes, which may complement its mapping. For instance, historical data to identify the parts of their supply chain most prone to disruption. Likewise, CTPs may draw upon pre-existing documents such as inventories of information and other associated assets in the relevant parts of their mapping.

Table 1: Illustrative non-exhaustive list of potential resources

Types	Examples
Data and Information	● customer firms' data ● open-source data ● proprietary data ● data analytics tools ● service level data
Facilities	● jurisdictions/regions from where systemic third party services are provided, including those where assets, such as data, belonging to firms are stored or processed ● premises used for the delivery of systemic third party services eg data centres (including whether they are owned by the CTP or co-located) ● backup and disaster recovery sites ● other relevant business premises
People	● departments, entities, and individual roles involved in the provision of systemic third party services to firms, including: (i) key departments and functions at the CTP; (ii) persons connected to the CTP; (iii) key Nth party providers; and (iv) managed service providers (MSPs) approved by the CTP.
Processes	● design and approval of systemic third party services ● assurance (including testing) of systemic third party services ● change management ● incident management plans (see below)
Supporting services	● Domain Name Systems (DNS) ● operations and maintenance ● security

	● Secure Sockets Layer (SSL) certificates
Technology	● Artificial Intelligence/Machine Learning models ● hardware ● software, including: (i) open source software; (ii) software owned by the CTPs or Persons Connected to the CTP; and (iii) software provided by key Nth Party suppliers. ● mapping of hardware, software and other technology resources should identify known concentrations and potential single-points-of-failure, and other significant risks
Supporting infrastructure	● cables ● cooling ● energy supply ● public telecommunications operators ● utilities (electricity, water) ● transport (air, shipping etc)

Requirement 7: Incident management

A CTP must effectively manage CTP operational incidents including by:

(1) implementing appropriate measures to respond to and recover from CTP operational incidents in a way that minimises the impact, or potential impact, on the stability of, or confidence in, the UK financial system;

(2) setting an appropriate maximum tolerable level of disruption to each systemic third party service;

(3) maintaining and operating an incident management playbook, the first version of which must be in place within 12 months of the CTP being designated by HM Treasury, which sets out the plans and procedures to be followed by the CTP in the event of a CTP operational incident in order to:(a) respond to and recover from the CTP operational incident; and

(b) facilitate effective communication with, and support to, the regulators and affected firms (individually and collectively); and

(4) cooperating and coordinating with the regulators and affected firms in response to CTP operational incidents, including through Collective Incident Response Frameworks.

6.30 Requirement 7 is vital for ensuring that CTPs manage potential systemic risks when responding to a CTP operational incident. It applies in addition, and without prejudice to, any individual support that a CTP may provide to affected firms during a CTP Operational Incident in line with their contractual commitments.

6.31 As noted in the 'The Bank of England's approach to enforcement statements of policy and procedure' and the FCA's equivalent in the FCA Handbook: Critical third parties (Statement of Policy) relating to Disciplinary Measures Instrument 2024, when deciding whether to take enforcement action against a CTP due to an alleged breach of its obligations by or under FSMA (including the CTP duties), the regulators will consider the nature, extent and effectiveness or likely effectiveness of any remedial action the CTP has taken or will take in respect of the breach and how promptly it was or will be taken. This may include but will not be limited to the adequacy of incident management measures taken by the CTP in accordance with the regulators' rules. This highlights the importance of a CTP implementing effective incident management measures, and regularly assessing their effectiveness to drive continuous improvement.

Response and recovery measures

6.32 A CTP may set out its incident response and recovery measures in a single or multiple documents, including:

- business continuity and disaster recovery plans;
- contingency plans;
- cyber-incident response plans (for cyber-incidents only); and/or
- crisis management and communication plans.

6.33 A CTP's response and recovery measures should cover the lifecycle of an incident, including but not limited to:

- the setting of an appropriate maximum tolerance for disruption for the systemic third party service ahead of a CTP Operational incident (see below);
- the classification of incidents based on predefined criteria eg expected recovery time and (if known) their potential impact on the CTP's customer firms. A CTP's incident classification should consider whether the incident:
    - warrants immediate and urgent action by specialist teams, management, senior management or the CTP's governing body; and
    - meets the definition of a CTP Operational incident, which will trigger the reporting requirements in section 8.

- a clear, communicated allocation of decision-making authority, responsibilities and roles within the CTP. A CTP should consider setting up an incident response group made up of appropriately skilled and senior individuals when there is a CTP operational incident

- procedures and targets for restoring systemic third party services and recovering assets;

- internal and external communication plans; and

- continuous improvement through the incorporation of lessons learned from exercises, historic incidents, near-misses and testing (see sections 7 and 8).

6.34 A CTP should also:

- periodically, and at least annually assess its response and recovery measures and update them as appropriate (see section 7); and
- take reasonable steps to identify the root causes of CTP operational incidents and address them as soon as practicable to reduce the risk of reoccurrence (see Section 7).

6.35 Where relevant, a CTP's response and recovery measures should cover CTP operational incidents with a potential cross-border and/or cross-sectoral impact.

Appropriate maximum tolerable level of disruption

6.36 A CTP's appropriate maximum tolerance for disruption should identify the timeframe and, if appropriate, other metrics within which the impacts of not resuming a systemic third party service would become unacceptable to the CTP in light of the Overall Objective.

6.37 A CTP's appropriate maximum tolerable level of disruption differs from but should fulfil a similar outcome to the impact tolerances that firms are required to set for their IBSs. In particular it should:

- provide a standard which a CTP's governing body, senior management and staff essential to the delivery of systemic third party services to firms should refer to when allocating resources, developing response and recovery measures etc.; and
- inform decision-making during a CTP operational incident.

6.38 When setting an appropriate maximum tolerable level of disruption for their systemic third party services, a CTP should assume that disruption will occur and not focus excessively on the cause or probability of disruption.

6.39 A CTP should use appropriate metrics and targets when setting an appropriate tolerance for disruption for its systemic third party services. It is up to the CTP to identify these metrics and targets. However, in doing so, it should:

- take into account the Overall Objective and the CTP duties;
- include at least one time-based metric;
- consider additional, non-time-based metrics if appropriate; and
- cover the end-to-end delivery of the systemic third party service in both:
    - business-as-usual; and
    - periods of heightened or peak activity. For instance, if the service is capable of failing over to a backup site, different availability zone or region, the CTP should consider the capacity of the relevant backup site, availability zone or region to cope with a sudden spike in activity or demand.

6.40 To inform the setting of an appropriate maximum tolerable level of disruption (and the regulators' periodic reviews of a CTP's systemic third party services (see section 3 of the CTP approach document)) a CTP should encourage firms to identify which of its services are key to the resilience of their IBSs, and where possible give the CTP an indication of the recovery times that these firms expect for those systemic third party services.

6.41 Once set, a CTP must share its appropriate maximum tolerable level of disruption for each systemic third party service with the firms it provides this service to.

6.42 A CTP's appropriate maximum tolerance for disruption should promote continuous improvement to the resilience of its systemic third party services. A CTP may agree stricter service levels in its contractual arrangements with firms and test their systemic third party services against these stricter service levels.

Incident management playbook

6.43 The term 'incident management playbook' is an umbrella term for any documented plans and procedures to be followed by the CTP in the event of a CTP operational incident in order to:

- respond to and recover from the CTP operational incident; and
- facilitate effective communication with, and support to, the regulators and affected firms (individually and collectively).

6.44 A CTP's incident management playbook may also set out how the CTP will communicate with and support other stakeholders impacted by a CTP operational incident or other incidents, such as customers outside the financial sector.

6.45 A CTP may refer to its incident management playbook by a different name internally. Where a CTP provides services to other sectors in addition to financial services, it is not required to produce a separate incident management playbook for its customer firms and may leverage its existing documented plans and procedures.

6.46 Regardless of the form it takes, a CTP's incident management playbook should deliver the following outcomes:

- promoting an effective response to the CTP operational incident, including by:
  - identifying the key people, teams and functions required for the CTP to respond and recover from the incident;
  - having a clear communications plan to deal with adverse coverage in mainstream and social media; and
- ensuring that the CTP has appropriate, documented, effective, and regularly assessed processes to communicate and cooperate with the regulators and the firms they provide systemic third party services to during a CTP operational incident.

6.47 Table 2 sets out a non-exhaustive list of areas that a CTP's incident management playbook should cover.

Table 2: Areas that a CTP's incident management playbook should cover

Impact Assessment	• How the CTP will assess the severity of incidents, including how it will decide whether they meet the definition of a CTP Operational Incident.
Escalation	• How the CTP will escalate CTP Operational Incidents internally, and to whom.
Allocation of responsibility	• How the CTP will allocate responsibility for responding to CTP operational incidents at technical, management and senior management levels; and • How the CTP will activate internal incident response procedures and convene response teams.
Communication with affected firms and the regulators	• How the CTP will communicate with affected firms and the regulators in an effective, prompt and secure manner during CTP operational incidents, including: (i) method(s) of communication eg blog posts, phone calls, SMSs, emails to customers' recovery accounts, incident notifications, online updates etc;

	(ii) the frequency with which the CTP will typically communicate; and (iii) the name of at least one Collective Incident Response Framework that the CTP will use to share information and assurance with affected firms collectively.
Support to affected firms and the regulators	• How the CTP will support affected firms, and the regulators to mitigate risks to the stability of, and confidence in, the financial system (eg by supporting their crisis communications if appropriate).
Public communications	• The CTP's approach for communicating publicly about CTP operational incidents where appropriate, including its general approach to: (i) addressing disinformation and misinformation relating to these incidents in mainstream and social media; and (ii) correcting and rectifying factual inaccuracies and out-of-date information previously disclosed.
Incident resolution	• The CTP's process for closing down its incident response procedures following the resolution of a CTP Operational Incident.

6.48 A CTPs' incident management playbook should ensure that affected customer firms and the regulators receive necessary data and information that is accurate and provided in a consistent and timely manner throughout the lifecycle of the incident, including on:

- the implementation of the CTP's response and recovery measures;
- parts of the CTP's supply chain affected by the incident; and
- general guidance that may assist:
  - the regulators in the exercise of their CTP functions; and
  - affected firms in responding to and recovering from the CTP operational incident. This guidance should be of general use to affected firms, and is additional to, but does not include any additional bilateral guidance that a CTP may provide confidentially to individual affected firms pursuant to the terms of contractual arrangements.

6.49 If the regulators consider that a CTP's incident management playbook does not meet the outcomes set out in their rules, the CTP will need to enhance, review or update it accordingly. A CTP's incident management playbook must comply with the regulators' requirements no later than 12 months from the CTP's designation by HM Treasury.

6.50 Although incident management playbooks seek to promote a consistent and coordinated response to CTP operational incidents, the regulators recognise that each incident is unique and there can be no one-size-fits-all approach.

6.51 A CTP should make its incident management playbook available to the regulators upon request.

Engagement with Collective Incident Response Frameworks

6.52 A CTP must cooperate with the regulators and affected firms to coordinate responses to CTP operational incidents, including through Collective Incident Response Frameworks.

6.53 The Bank's webpage on Operational resilience of the financial sector mentions some of these Collective Incident Response Frameworks, [25] which include:

- the **Authorities' Response Framework** (ARF)[26], which is a formal way for UK financial authorities (the regulators and HM Treasury) to co-ordinate with each other when there is an incident or threat that could cause a major disruption to financial services; and
- the Sector Response Framework (SRF), which is owned and maintained by the Cross-Market Operational Resilience Group (CMORG).

6.54 For the purposes of Requirement 7, 'cooperating' involves a CTP using pre-agreed, documented, and appropriately rehearsed ways to communicate with and support one or more Collective Incident Response Frameworks during a CTP operational incident, so that it can provide appropriate updates and collective support to affected firms and the regulators. A CTP should cooperate with Collective Incident Response Frameworks:

- regularly in preparation of a potential future CTP Operational Incident, including (if appropriate) through incident management playbook exercises (see section 7);
- during a live CTP operational incident; and
- after the resolution of a CTP operational incident to agree and embed lessons learnt and remediation actions.

6.55 The regulators do not require a CTP to cooperate with any single Collective Incident Response Framework to the exclusion of others. A CTP must cooperate with at least one such framework but may cooperate with more than one. The frameworks referred to above are non-exhaustive. Additional frameworks could be created in the future. Given the potential cross-border impact of CTP Operational Incidents, a CTP may also cooperate with similar frameworks outside of the UK or covering multiple jurisdictions. Where this is the case, it should list all relevant collective incident management frameworks it cooperates with in its incident management playbook.

---

25 Operational resilience of the financial sector: **www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector**.

26 **https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/co-ordinating-the-response-to-disruption-of-financial-services**.

Requirement 8: Termination of services

A CTP must have in place appropriate measures to respond to a termination of any of its systemic third party services (for any reason), including by putting in place:

(1) arrangements to support the effective, orderly and timely termination of that service, and (if applicable) its transfer to another person, including the firm the service is provided to; and

(2) provision for ensuring access to, recovery and return of any relevant firm assets to each firm it provides that service to and (where applicable) in an easily accessible format.

6.56 Termination of a CTP's services may happen for various reasons, including but not limited to:

- a change of control;
- a corporate reorganisation;
- insolvency;
- legal, political, and regulatory issues; or
- a CTP operational incident from which the CTP cannot recover.

6.57 For the purposes of Requirement 8, insolvency includes all insolvency proceedings that may affect a CTP's ability to continue delivering systemic third party services including but not limited to a company voluntary arrangement (CVA), administration, receivership, and liquidation. It also includes insolvency proceedings outside the UK. Where termination is due to an insolvency, Requirement 8 continues to apply. However, a court-appointed insolvency practitioner may apply for a waiver or modification of this rule or any aspects thereof it wishes to disapply (subject to the relevant statutory tests being met).[27] In any event, the actions that a CTP is required to take under Requirement 8 should take place as part of its insolvency planning during business-as-usual, prior to any actual insolvency.

27 See **S138A of FSMA, https://www.legislation.gov.uk/ukpga/2000/8/section/138BA S138BA of FSMA**, and **The Prudential Regulation Authority's approach to rule permissions and waivers**, available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2024/july/pra-approach-to-rule-permissions-and-waivers-statement-of-policy.

6.58 Legal, political, and regulatory issues include legislative or regulatory changes, supervisory or enforcement action (including the imposition of disciplinary measures), judicial rulings, sanctions etc.

6.59 As noted in section 4, firms remain responsible for complying with applicable requirements and expectations on operational resilience, and outsourcing, and third party risk management, including in relation to stressed exit strategies. Requirement 8 seeks to ensure that CTPs facilitate firms' compliance with these requirements but does not replace them. Facilitating in this context means for a CTP to:

- develop and maintain plans covering the potential termination of its systemic third party services, which should be made available to firms that use these services to assist them in the development of their own exit plans; and

- providing reasonable support to firms following the termination of a systemic third party service, and during an appropriate transitional period thereafter. For instance, by not putting in place undue barriers, which disrupt or discourage the orderly termination of these services, or their transfer. However, facilitating does not extend to a requirement or expectation on a CTP to transfer ownership or grant use of its intellectual property eg proprietary services or technology, to another provider or to firms beyond what is necessary to enable an orderly termination and transition.

6.60 CTPs should interpret the phrase 'in an easily accessible format' as being limited to actions within their reasonable control. For instance, if a CTP stores data encrypted by a firm, and that firm has sole control of the encryption keys, Requirement 8 does not require the CTP to decrypt the data prior to returning it to the firm.

7: Self-assessments, Scenario-testing, Incident Management Playbook Exercises, and other assurance

7.1 This section outlines how the regulators expect CTPs to comply with the information-gathering and testing requirements in:

- s312P of FSMA;

- chapters 5-7 of the Critical third parties sourcebook in the FCA Handbook; and

- The following chapters in the Critical third parties Parts of the PRA Rulebook, and Bank of England FMI Rulebook:
    - general evidence requirement, scenario-testing and incident management playbook exercises;
    - self-assessment; and
    - information-sharing with firms.

General evidence requirement

7.2 A CTP must be able to demonstrate to the regulators its ability to comply with their rules (referred to as the 'general evidence requirement'). It must do so through a combination of:

- regular, mandatory:
    - self-assessments;
    - scenario-testing; and
    - incident management playbook exercises; and
- providing the regulators with information upon request.

Self-assessment

7.3 A CTP must provide to the regulators:

- within three months of the CTP being designated by HM Treasury, an interim self-assessment; and
- annually thereafter, an annual self-assessment.

7.4 A CTP must keep a copy of the interim and each annual self-assessment for a period of at least three years after submitting them to the regulators.

Interim self-assessment

7.5 Although the information that CTPs should include in the interim and annual self-assessments is identical, an interim self-assessment fulfils a unique and essential purpose, which is for the regulators to:

- get an early indication of the extent to which a CTP is able to meet the regulators' rules at the point of designation by HM Treasury; and
- identify areas to prioritise in the early phase of oversight.

7.6 A CTP's interim self-assessment is a tool for the regulators to diagnose and benchmark a CTP's compliance with the CTP duties upon designation, in order to make their subsequent oversight of that CTP more risk-based, resource-efficient and targeted.

Common expectations for interim and annual self-assessments

7.7 Self-assessments should set out the CTP's analysis of how it has met the CTP duties. In line with Requirement 1, the regulators expect the self-assessment to undergo appropriate internal review and approval before a CTP submits it to them (see section 6).

7.8 A CTP should ensure that its self-assessments are clear and concise. The information in Box 2 below is not exhaustive. A CTP may provide additional evidence if it believes it can help demonstrate that it is complying with the regulators' rules.

7.9 The CTP should make information referenced in its self-assessments (eg audit reports, certifications, test results etc) available to the regulators upon request, but does not need to include all this supporting information when it submits its self-assessments.

7.10 In line with CTP Fundamental Rule 6, a CTP's self-assessments should be balanced, thorough and transparent. They should openly highlight identified areas for improvement and any proposed remediation. CTPs should use factual language and avoid an excessive 'good news culture' in their self-assessments.

7.11 The quality of self-assessments should improve over time in line with a CTP's evolving understanding of the CTP duties.

Box 2: Information for CTPs to include in their self-assessments [28]

Governance: demonstrate how the CTP's governance arrangements support its risk management and ability to prevent, respond, and adapt to, as well as recover from a CTP operational incident. CTPs should highlight how its clear lines of accountability and channels of communication enable this and explain any significant relevant organisational changes over the past 12 months.

Risk management: demonstrate how the CTP's risk management framework and processes allow it to manage risks to its delivery of systemic third party services, including the ability to identify and escalate operational and financial risks. The CTP should also explain any changes to its risk management framework and policies over the past 12 months.

Supply chain: demonstrate how the CTP is effectively managing risks to its supply chain. The CTP should provide examples to demonstrate the due diligence it undertook, and the

28 The purpose of the self-assessment is for the CTP to demonstrate compliance with all the CTP duties. The information in Box 2 aims to ensure that CTPs provide this information in a comparable, consistent and structured manner.

initial and ongoing assurance received from Key Nth Party Providers to help manage relevant risks.

Cyber and technology: demonstrate how the CTP is effectively identifying and managing risks to its technology and cyber resilience. In doing so, the CTP should consider risks relating to people, processes, technology, and information insofar as they might impact the cyber resilience of the systemic third party services it provides. The CTP should also show how its cyber resilience and security measures allow its technology to support, deliver, and maintain any systemic third party services. The CTP should also highlight relevant testing conducted over the past 12 months and explain any proposed future steps to further enhance its cyber resilience.

Change management: demonstrate how the CTP's approach to ensuring that significant changes to the processes and technologies used to deliver systemic third party services are planned, decided, implemented, and operating effectively. This should include an overview of the CTP's contingency planning processes for responding to changes that do not meet their intended outcomes and could have a potential to give rise to CTP operational incidents.

Mapping: demonstrate how the CTP has used mapping to:

- identify resources and vulnerabilities; and
- inform scenario testing to mitigate the identified vulnerabilities.

Incident management: demonstrate how the CTP effectively manages CTP operational incidents. Specifically, a CTP should show how its incident management playbook can be used to mitigate risks to its customer firms and the wider impacts stemming from incidents that may adversely affect a CTP's systemic third party services. A CTP should also provide an update on the implementation of any recommendations in the after-action report that followed its most recent test of the playbook. In addition, the CTP should explain it has relevant measures in place to allow it to respond and recover from CTP operational incidents in a way that minimises the impact.

Termination: demonstrate that the CTP has appropriate measures in place to respond to a termination of its systemic third party services, including by setting out:

(i) transitional arrangements to support the effective, orderly, and timely termination of those services, and if applicable their transfer;
(ii) provision for access, recovery and return of relevant assets (including data) to firms; and
(iii) evidence that the CTP can maintain the ongoing delivery of systemic third party services through a termination and transition of services.

The CTP should draw on examples (actual or hypothetical) to illustrate how it would support firms in the event of a termination of its systemic third party services.

Scenario testing: describe the CTP's strategy for testing its ability to deliver systemic third party services within its appropriate maximum tolerable level of disruption in severe but plausible scenarios and how it fits into its broader approach of enhancing the resilience of its services. The CTP should explain how it has gained assurance through the selected scenarios and types of testing used. It should also specify any scenarios under which the CTP could not continue to provide the systemic third party services within its appropriate maximum tolerable level of disruption (see paragraphs 7.12 to 7.23).

Lessons learned: set out lessons learned from all types of testing, exercises and CTP operational incidents, and demonstrate they have been fully embedded. A CTP should also describe any actions taken or planned to address any issues and risks identified.

Scenario-testing and Incident Management Playbook Exercises

(a) Scenario testing

7.12 As part of its obligation under the general evidence and information requirement, a CTP must carry out regular scenario testing of its ability to continue providing each systemic third party service within its appropriate maximum tolerable level of disruption in the event of a severe but plausible disruption to its operations. A CTP may perform its scenario testing against stricter thresholds in addition to its appropriate maximum tolerable level of disruption.

7.13 When carrying out scenario testing, a CTP must identify an appropriate range of adverse circumstances of varying duration, nature and severity relevant to its business, risk profile and supply chain and consider the risks to the delivery of the systemic third party service in those circumstances.

7.14 If a CTP does not already have an appropriate scenario-testing programme at the point of designation, it should implement such a programme and carry out its first scenario tests no later than 12 months following designation by HM Treasury. If the CTP already conducts scenario-testing, it should adapt it to meet the regulators' requirements and expectations (where required) no later than 12 months following its designation. Thereafter the CTP must conduct regular scenario tests, which should be at least annual, but might be more frequent if the CTP deems it appropriate, or if the regulators request or direct it. For instance, if a new risk or threat to the resilience of a CTP's systemic third party services is discovered or emerges rapidly and unexpectedly, a CTP should carry out a scenario test to assess its ability to respond and recover from this new risk or threat.

7.15 A CTP's scenario testing should:

- assume that disruption has occurred and not focus on preventing incidents from occurring or considering the relative probability of them occurring. This does not prevent a CTP from taking preventative actions to minimise the risk of CTP operational incidents occurring and assessing the effectiveness of these preventative controls in line with Requirement 2 (see section 6); and
- complement and draw on other testing undertaken by the CTP including business continuity and disaster recovery testing etc.

Scenario selection

7.16 A CTP's scenario selection should take into account how systemic third party services are delivered, informed by the end-to-end mapping of these services and the resources which deliver, support and maintain each service. For instance, potential single-points-of failure which the CTP has identified in its supply chain in its mapping, or other processes.

7.17 A CTP's scenario testing should regularly include one or more scenarios involving CTP operational incidents relating to:

- supply chain eg disruption to a service provided by a Key Nth Party Provider that is essential to the delivery of a systemic third party service;
- loss or reduced provision of technology underpinning the delivery of systemic third party services;
- deletion, manipulation or compromise of assets, including data, essential to the delivery of systemic third party services. For instance, as a result of a ransomware attack, or the actions of a malicious insider;
- unavailability of:
    - facilities impacting the delivery of systemic third party services;
    - key individuals and groups; and
    - systems;
- disruption to the CTP's energy supply, key infrastructure and networks (eg national communications networks); and
- disruption taking place during a historic, hypothetical or planned change management programme or major update.

7.18 A CTP may use a range of sources to inform their scenario selection, including but not necessarily limited to:

- incidents and near-misses at the CTP and its peers;
- risks identified in its mapping under Requirement 6 (see Section 6) and other relevant tools (eg internal risk registers, threat intelligence etc)
- scenarios derived from the government's National Risk Register, and equivalent non-UK registers;
- threat intelligence based on the National Cyber Security Centre (NCSC)'s sector threat assessments, and threat intelligence from equivalent non-UK bodies, such as cyber-security authorities in its home jurisdiction, or other jurisdictions where it operates;
- scenario libraries or suggested scenarios maintained by Collective Incident Response Frameworks; and
- any other source that the CTP believes to be relevant in the design of the scenarios.

7.19 A CTP is accountable and responsible for identifying the scenarios it will test. However, it should share details of the scenarios it proposes to test (including their relevance to the overall objective of the CTP regime, their plausibility and their severity) in advance with the regulators, the firms it provides systemic third party services to, and the Collective Incident Response Frameworks referred to in section 6.

7.20 In addition to any scenarios identified and tested by the CTP in compliance with the requirements in the previous section, a CTP should test certain scenarios if requested to do so by the regulators (see CTP approach document) and on the timeline indicated by the regulators.

Severe but plausible

7.21 Severe but plausible scenarios should comprise scenarios that truly test a CTP's ability to deliver systemic third party services. When assessing plausibility, CTPs should consider whether the relevant scenario is consistent with events known to have occurred in the past ie, it has a basis in prior knowledge. It is also reasonable to extrapolate prior events to reflect known trends in the threat landscape or other external factors.

7.22 Whilst the scenario should not be so remote that it becomes meaningless or impractical to respond to, a CTP should focus on the severity and the significance of the impact resulting from its chosen scenarios. Scenarios should be demanding in testing the resilience of a CTP and should also help it test the boundary of its ability to recover systemic third party services in line with its appropriate maximum tolerable level of disruption (or other, stricter metrics). The most severe but still plausible scenarios may call into question the CTP's financial or operational viability. The range of scenarios tested should also seek to explore differing aspects of the resilience of the CTP (eg service

continuity, cyber-resilience, management of insider threats and supply chain risks etc) as well as the associated recovery processes.

7.23 Where appropriate, a CTP should test a single scenario multiple times adjusting its severity within the confines of plausibility (including the most severe but plausible scenario identified) through the addition of relevant complicating factors that may make the scenario more demanding in terms of recovery. A CTP's maps and other tools can assist in this process. A CTP could adjust the severity of a scenario in one or more of the following ways:

- increasing the number or type of systemic third party services, or resources supporting those services that become unavailable;
- increasing the period for which systemic third party services, or resources supporting those services remain unavailable;
- running the scenario at times of peak activity, out of regular business hours or during common or public holiday periods;
- running the scenario during system migration, major upgrades or updates; and/or
- adding other complicating factors such as adverse media coverage, disinformation or misinformation relating to the incident, disruption to the CTP's energy supply, extreme weather etc.

(b) Incident management playbook exercise

7.24 As part of the general evidence requirement, a CTP must assess the effectiveness of its incident management playbook regularly, including undertaking appropriate incident management playbook exercises with a representative sample of the customer firms to which it provides systemic third party services. A CTP must carry out the first of these exercises within the first twelve months of designation by HM Treasury, and at least biennially thereafter. The regulators may request or direct a CTP (using their powers under s312N FSMA) to carry out incident management playbook exercises earlier or more frequently than biennially if appropriate. For instance, to ensure that the CTP has appropriately embedded lessons learnt from a CTP operational incident.

7.25 Incident management playbook exercises are vital for a CTP to manage risks to the stability of, or confidence in, the UK financial system arising from the failure or disruption to its systemic third party services. The main aim of these exercises is for a CTP to assess whether its incident management playbook is effective, and progressively improve it by deploying it in a scenario-based, simulated CTP operational incident with a sample of the firms that the CTP provides systemic third party services to. These exercises promote a collaborative approach that should progressively improve the way a CTP communicates with and supports affected firms during a CTP operational incident.

7.26 The collaborative nature of incident management playbook exercises distinguishes them from other exercises and tests that a CTP may carry out. For instance, in line with recognised standards, CTPs may already maintain an exercise programme to validate the effectiveness of their business continuity strategies and solutions. However, CTPs tend to run these exercise programmes internally, with the only external input being that of an external auditor in certain instances. Internally run exercises do not allow a CTP to get feedback on how to improve its incident management playbook from the firms that would be impacted by a CTP operational incident. Similarly, some CTPs allow their customers to perform various forms of testing on assets (applications, data) belonging to those customers but stored by the CTP. While this type of testing is key to ensure that firms configure and use a CTP's services resiliently, it does not involve active collaboration between a firm and a CTP.

Participation by firms, the regulators and other stakeholders

7.27 The regulators' rules for firms do not require them to participate in the incident management playbook exercises of the CTPs they receive systemic third party services from. However, it is consistent with their regulatory obligations on operational resilience, and outsourcing and third party risk management,[29] as well as in their own interest. This is particularly the case if the CTP carrying out the exercise, and the systemic third party service(s) on whose disruption the exercise is based are core to a firm's delivery of one or more important business services. It is also necessary for incident management playbook exercises to achieve a critical mass of participating firms to be effective. The 'G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector' endorse the idea of joint exercises involving firms and CTPs as a means of evaluating the adequacy of firms' response and recovery measures.[30]

7.28 A firm may scale its level of participation at a CTP's incident management playbook exercise depending on factors such as:

- its systemic significance;
- whether it is internationally active;
- the resources it can commit to the exercise;
- the importance of the systemic third party service on whose disruption the exercise is based to the delivery of the firm's important business services;

29 See, for instance SS1/21 **SS1/21 'Operational resilience: Impact tolerances for important business services'** para 6.13, and **SS2/21 'Outsourcing and third party risk management'** Section 10.

30 February 2023: **https://www.gov.uk/government/publications/g7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector**.

- the number of CTPs that provide services to that firm that are carrying out incident management playbook exercises that year; and their relative importance to the firm's delivery of important business services.

7.29 Participation by a firm in an incident management playbook exercise will typically involve:

- attending the exercise;
- considering the quality and timeliness of information and support provided by the CTP during the exercise; and
- providing feedback to the CTP, collectively with other participating firms, on suggested improvements to the above. Some firms may choose to participate more actively in the incident management playbook exercise or specific aspects, such as scenario selection, planning and execution etc.

7.30 Although CTPs are responsible for running their incident management playbook exercises, they can use outside support in the design and execution of these exercises. For instance, Collective Incident Response Frameworks or independent experts (eg consultants or external testers), both of which can help coordinate participation by firms and assist with scenario selection, logistics, follow-up etc.

7.31 Depending on the objectives of the exercise, the chosen scenario and discussions with the regulators and participating firms, a CTP should involve other stakeholders to the extent appropriate including, but not necessarily limited to:

- persons connected to the CTP;
- key Nth Party Providers; and
- the regulators and other authorities (in an observing capacity).

Objectives and types of incident management playbook exercise

7.32 The expectations in the previous section on how CTPs should approach scenario selection in the context of the scenario-testing requirements in the regulators' rules apply equally to the selection of scenarios on which to base incident management playbook exercises.

7.33 While all incident management playbook exercises share the overarching aims described above, CTPs (following discussion with participating firms and the regulators) may set one or more granular objectives for each exercise. These granular objectives, which are neither exhaustive nor mutually exclusive, may include:

- exploring how the playbook could facilitate the response to a new or emerging risk;
- examining in detail whether the playbook, or parts thereof, are fit-for-purpose to respond to a specific risk;
- testing the playbook, or parts thereof on a pass/fail basis;

- rehearsing a part of playbook that has generally been proven effective, but not fully tested; and
- practising a part of the playbook that has been proven effective and fully tested.

7.34 There are different types of incident management playbook exercise, some of which are summarised in the 'G-7 Fundamental Elements of Cyber Exercise Programmes'.[31] A CTP is responsible for selecting the most appropriate type of exercise ahead of its next scheduled exercise, and should discuss its choice with the regulators, and participating firms. When choosing an appropriate exercise, a CTP should consider:

- the overall aims, and specific objective(s) of the exercise;
- the systemic third party service(s) whose disruption will form the basis of the scenario;
- the suitability of the chosen scenario(s);
- any prior feedback on the effectiveness of its incident management playbook from the:
    - the regulators;
    - the firms it provides systemic third party services to;
    - Collective Incident Response Frameworks;
    - other relevant stakeholders eg other authorities, independent experts;
- the CTP's confidence in its incident management playbook, and any evidence it can provide to substantiate this confidence;
- lessons learnt and areas for improvement identified through prior exercises, previous incidents etc, and the extent to which they have been implemented;
- risks identified through its mapping, supply chain risk management and other processes (see Section 5);
- the cost, timing and resource implications of different types of exercise. CTPs should cycle between light-touch and intensive exercises and not choose the most light-touch option each time; and
- number of expected participating firms.

Follow-up to incident management playbook exercises

7.35 At the end of an incident management playbook exercise, a CTP should collate feedback from participating firms and (where relevant) the regulators on how to improve its incident management playbook.

7.36 A CTP must, as soon as is practicable, prepare and submit to the regulators a report of its latest incident management playbook exercise (including any actions taken in light of

---

31 December 2020:**https://assets.publishing.service.gov.uk/media/5fe4852c8fa8f56af53c5d77/G7_Fundamental_Elements_of_Cyber_Exercise_Programs_October_2020.pdf**.

the results of that exercise). A CTP's annual self-assessment should also include this report.

7.37 A CTP should update the regulators on the implementation of any changes to its incident management playbook in response to feedback to its latest incident management playbook exercise no later than six months after the date of its most recent exercise.

Information provided by CTPs to the Regulators

7.38 In addition to the self-assessment, scenario testing and incident management playbook requirements examined above, a CTP must comply with requests by the regulators for information reasonably required in connection with the exercise of their CTP oversight functions (S312P of FSMA). The regulators' statutory information-gathering powers also empower them to require information from a Person Connected to a CTP.

Audit reports, certifications etc

7.39 CTPs should provide the regulators with independent assurance reports or certifications of compliance with recognised standards upon request. However, audit reports, certifications etc have limitations. In particular, they tend to verify the existence of certain controls. Therefore, they can be of limited use for certain purposes, such as understanding how a CTP would deal with a specific scenario. For instance, a recognised certification or standard may confirm that a disaster recovery policy exists and is regularly tested but may not provide evidence of the effectiveness or rigour of any testing undertaking (including whether it considered potential systemic risks), or the ability of the CTP to respond to a specific disruptive scenario or class of scenarios. Certifications and standards, therefore, provide helpful confirmation as to the design of certain controls but not necessarily on their effectiveness. A CTP should not assume nor expect that the mere provision of audit reports, certifications etc will give the regulators all the information and assurance they require in all cases.

Results of CTPs' internal tests and incident management playbook exercises

7.40 A CTP should share information with the regulators relating to tests and exercises not explicitly mandated by their rules upon request. The information shared should be proportionate to the objectives of the oversight regime for CTPs. A CTP should take reasonable steps to remove restrictions on its ability to share this information with the regulators, including where the tests were performed, supported, or validated by independent parties.

Information provided to other authorities

7.41 CTPs should share information provided to other authorities that carry out similar functions or have overlapping mandates over CTPs (including the results of tests

performed by or on behalf of these authorities) upon request by the regulators. The term 'other authorities' includes:

- non-UK financial regulatory, oversight or supervisory authorities, such as (where applicable) the CTP's lead overseer under DORA;
- regulators and other public authorities outside the financial services sector, which may have an overlapping mandate or interest in respect of the CTP.

7.42 The CTP approach documents sets out the circumstances in which the regulators may ask a CTP for information provided to other authorities, and how they will ensure that these requests are subject to appropriate safeguards. However, sharing this information is likely to be in the CTP's own interest, as it can reduce the need for more resource-intensive forms of oversight by the regulators that could duplicate oversight already undertaken by other authorities.

7.43 A CTP should make this information available to the regulators subject to the other authorities' consent, where such consent is legally required.

Collaborative or industry-wide testing

7.44 A CTP may be subject to or take part in collaborative or industry-wide testing and exercises by firms.

7.45 A CTP should make available to the regulators upon request the results of relevant collaborative or industry-wide exercises and tests it participates in. CTPs should take reasonable steps to ensure that any agreements governing these tests, exercises etc, including contractual arrangements, and non-disclosure agreements (NDAs) do not prevent or limit the sharing of information with the regulators for performing their functions. This includes taking reasonable steps to ensure that the sharing of this information with the regulators does not expose the CTP to potential liability in damages.

Sharing of assurance and testing information with firms

7.46 A CTP must have in place effective and secure processes and procedures to ensure sufficient and timely information is given to firms to which it provides any systemic third party services to enable them to manage adequately risks related to its use of the CTP's systemic third party services. A CTP should share time-sensitive information as soon as practicable. For instance, information about a new issue, risk or threat that may require remediation, risk mitigation or risk management from these firms.

7.47 The specific information that a CTP must share with the firms they provide systemic third party services pursuant to the regulators' rules to includes:

- results of testing and exercises performed in compliance with the regulators' rules, including any action taken in the light of the results these tests and exercising;
- the annual self-assessment submitted to the regulators, redacted as appropriate (but not the interim self-assessment); and
- the appropriate maximum tolerable level of disruption of each systemic third party service it provides to that firm.

7.48 A CTP should redact information which they consider should be for the regulators only from the version of the self-assessment shared with the firms it provides systemic services to. However, the redacted text should not undermine the CTP's obligations mentioned above.

7.49 To comply with the requirement above, a CTP must also provide to firms information not explicitly mentioned in the regulators' rules, which may assist firms in managing risks related to their use of the CTP's systemic third party services. A CTP should adopt a 'transparency by default' approach with regards to this requirement. Examples of relevant information include, but are not limited to, summaries (prepared by the CTP) of key, relevant findings from skilled persons reviews, and any remediation that the CTP proposes to undertake in response. When sharing relevant information with firms, the regulators recognise that there may be confidentiality and sensitivity issues to be taken into account.

7.50 A CTP is responsible for developing an appropriate method for sharing information with relevant firms. This method should include controls to ensure that confidential or sensitive information is appropriately protected against unauthorised parties. A CTP may use existing or purpose-built mechanisms, such as portals or databases, where relevant firms can access data and information that CTPs are required to share with them under the CTP duties.

Skilled person reviews

7.51 As noted in section 3, the regulators' approach to the exercise of their powers to order skilled persons reviews of CTPs are set out in:

- chapters 12 and 13 of the Critical third parties sourcebook in the FCA Handbook;
- the 'Contracts with Skilled Persons and delivery of reports' chapter in the Critical third parties Part of the PRA's and Bank's Rulebooks; and
- Joint Bank/PRA SS7/24 – Reports by skilled persons: Critical third parties.

8: Incident Reporting and Notifications

8.1 This section sets out how CTPs should comply with the requirements to report CTP operational incidents in:

- the 'Incident Reporting', 'Notifications' and 'Inaccurate, False or Misleading Information' chapters in the Critical third parties parts of the PRA Rulebook, and the Bank of England FMI Rulebook, and
- chapters 8-10 of the Critical third parties sourcebook in the FCA Handbook.

8.2 The incident reporting requirements on a CTP apply in addition and without prejudice to:

- the requirements in CTP Fundamental Rule 6; and
- any information and support that a CTP provides bilaterally and confidentially to individual affected firms in line with its contractual obligations.

8.3 The incident reporting requirements on a CTP complement the requirements on firms. In particular, they seek to ensure that affected firms have appropriate, consistent and timely information about CTP operational incidents to:

- assess the impact on their ability to meet applicable requirements;
- fulfil their incident reporting and notification obligations to the regulators; and
- withstand, respond to, recover and learn from these incidents, individually and collectively.

8.4 These incident reporting requirements on a CTP also seek to enable the regulators to form a complete picture of the impact of CTP operational incidents on their objectives and react accordingly, including deciding whether to invoke the ARF, and coordinate with other authorities and regulators in the UK and overseas.

8.5 As noted in the Bank of England's CTP Enforcement SoP and the FCA's equivalent set out in the FCA Handbook: Critical third parties (Statement of Policy) relating to Disciplinary Measures Instrument 2024, when deciding whether to take enforcement action against a CTP due to an alleged breach of its obligations by or under FSMA (including the CTP duties), the regulators will consider how promptly, comprehensively and effectively the CTP brought the breach to the attention of the regulators, any other relevant regulatory authorities or law enforcement agencies and/or any affected firms. This includes situations where the CTP's alleged breach resulted in a CTP operational incident and highlights the importance of a CTP complying with the letter and the spirit of the incident reporting and notification requirements in the regulators' rules and this section.

CTP operational incident

8.6 The incident reporting requirements apply to a CTP operational incident which, as section 2 notes, means either a single event or a series of linked events that:

- causes serious disruption to the delivery of a systemic third party service; or
- impacts the CTP's operations such that the availability, authenticity, integrity or confidentiality of assets belonging to firms which a CTP has access to as a result of it providing a systemic third party service to those firms is or may be seriously and adversely impacted.

8.7 CTPs are only required to comply with the requirements in the incident reporting rules in respect of incidents with an actual impact on one or both of the elements referred to in a para 8.6, not events with a potential, uncrystallised impact. They are not required to report incidents that do not cause such an impact ('near-misses'). However, a CTP should:

- in line with CTP FR 6, make the regulators aware of incidents that have not, at the time, caused such an impact but are highly likely to do so imminently or in the short-term;
- include aggregate data on near-misses and incidents not meeting the threshold for a CTP operational incident in their self-assessments. The regulators are particularly interested in areas for improvement and other lessons that a CTP has learnt from these near-misses, as well as any commonalities and trends in these near-misses.

8.8 The definition of CTP operational incident has two elements. The first element applies to incidents that seriously disrupt the delivery of a systemic third party service. As noted in section 2, 'disruption' should be interpreted purposefully in light of the Overall Objective, and includes (in relation to a systemic third party service) the:

- complete or partial failure of that service;
- complete or partial degradation to the quality of that service;
- complete or partial unavailability of that service; or
- service not performing as intended as a whole or in part.

8.9 A CTP should treat all events that disrupt a systemic third party service beyond its appropriate maximum tolerable level of disruption as causing 'serious' disruption for the purposes of the definition of a CTP operational incident but may set stricter thresholds. When assessing whether an incident meets the seriousness threshold of a CTP operational incident, a CTP should also take into account:

- its internal assessment and classification of the incident; and
- whether the incident warrants immediate and urgent action, including but not limited to escalation to specialist teams, senior management, the CTP's governing body etc.

8.10 The second element of the definition of CTP operational incident applies to situations, such as certain cyber-attacks, where the:

- CTP's operations are impacted; and
- there is not necessarily a serious disruption (as defined above) to a systemic third party service; but
- the impact on the CTP's operations does or may seriously and adversely impact the confidentiality, integrity, authenticity or availability of assets belonging to firms which the CTP has access to as a result of it providing a systemic third party service to those firms.

8.11 The second element of the definition of a CTP operational incident recognises that, depending on the CTP and the systemic third party service(s) it provides, a CTP may not know whether assets belonging to its customer firms have been affected by a compromise to its operations and, if so, which assets and to what extent. Customer firms retain certain responsibilities for protecting their assets when they place them on a CTP's infrastructure, eg with regard to the classification and encryption of data. Nevertheless, it is essential that a CTP promptly notifies the firms it provides systemic third party services to and the regulators of events impacting its operations that may have exposed the confidentiality, integrity, authenticity or availability of assets belonging to these firms to serious and adverse impact. This enables the firms to assess the impact of this breach, which in some instances may not lead to crystalised risks until later. For example, in 'harvest now, decrypt later' cyber-attacks.

Phased approach to incident reporting

8.12 A CTP must provide in each case to the firms that receive the affected service, and the regulators:

- an initial report;
- where required, one or more intermediate reports; and
- a final incident report.

8.13 A CTP must also provide additional information about the CTP operational incident to the regulators if requested under S312P of FSMA.

8.14 As noted in the regulators' rules, a CTP must take reasonable steps to verify the information in their incident reports ahead of submitting them. However, in the case of initial and intermediate incident reports in particular, when assessing what is reasonable in this context, a CTP should balance the competing needs to provide detailed information against the need to report to the regulators and affected firms early enough for them to assess the potential impact and severity of the incident and consider whether further action is warranted.

8.15 A CTP should use its incident management playbooks and its engagement with Collective Incident Response Frameworks under Requirement 7 in section 6, to ensure that incident reports reach all affected firms in a consistent, resource-efficient, and timely manner.

Format of incident reporting

Voluntary template for reporting of CTP operational incident

8.16 A CTP may use a range of formats for reporting a CTP operational incident to the regulators and firms as long as they include all the information required by the regulators' rules.

8.17 A voluntary template (including instructions) will be provided in due course. When available, CTPs may use this template to report CTP operational incidents to the regulators.

Incident reports submitted to other authorities

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

- non-UK financial regulators;
- UK non-financial authorities eg:
  - the Information Commissioner's Office (ICO)[32] under the Network and Information Systems (NIS) Regulations 2018[33] or Data Protection Act 2018[34] (and future versions thereof); and
  - the National Cyber Security Centre (NCSC);[35]
- its non-UK firm customers eg notifications to US banks under the Computer-Security Incident Notification rule.[36]

32 **www.ico.org.uk.**
33 **www.legislation.gov.uk/uksi/2018/506**.
34 **www.legislation.gov.uk/ukpga/2018/12/contents/enacted**.
35 **www.ncsc.gov.uk**.
36 **www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-55.html**.

- in some cases, the public at large eg in the case of US listed companies, the Securities and Exchange Commission's 'Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure' rule.[37]

Initial Incident Report

8.19 A CTP must, as soon as is practicable after the occurrence of a CTP operational incident and in so far as it is aware at the time of submission, submit separate initial incident reports to affected firms and the regulators containing the information in Table 4.

Table 4: Information in a CTP's initial incident reports

Information that must be provided to the regulators and affected firms	**Additional information that must be provided to the regulators only**
(1) a description of the CTP operational incident, which should include: (i) the nature and extent of: - the disruption to the systemic third party services eg complete or partial service failure, service(s) not performing as intended etc; or - impact to the CTP's operations; (2) the time when the incident was detected and if different, the local time in the location where the CTP operational incident was detected; (3) the name and number of systemic third party services affected; and *(4)* the geographical area, including the jurisdictions affected by the CTP operational incident; (5) if known, the cause of the CTP operational incident; (6) contact details of any individual who is responsible for communicating with the affected firms about the CTP operational incident;[38] (7) details of any initial action taken or planned in response to the CTP operational incident;	(10) the names of affected firms;[39] (11) the names of any other regulatory bodies or authorities that have also been notified of the CTP operational incident; and (12) any other relevant information that the CTP reasonably considers will assist the regulators in making an initial assessment of the potential impact of the CTP operational incident on the stability of, or confidence in the UK's financial system.

37 **https://www.sec.gov/newsroom/press-releases/2023-139**

38 This should include communicating with the Financial Sector Incident Response Frameworks in section 6.

39 Where known, the CTP should name individual firms as granularly as possible. However, the regulators recognise that a CTP may have a third party arrangement with a specific entity in a firm's group (such as an intra-group service provider, or a parent company) and may only be able to name the contracting entity.

(8) the anticipated amount of time it will take to resolve the CTP operational incident, including the anticipated recovery time for each systemic third party service affected; and (9) any other relevant information the CTP reasonably considers relevant to the affected firms and the regulators in making an initial assessment of the CTP operational incident's potential impact on affected firms.	

8.20 If there is a conflict between the level of detail in a CTP's initial report and the timeliness of the submission of that report to affected firms and the regulators, the CTP should prioritise timeliness and provide additional detail as necessary. When providing details of the time when the incident was detected, a CTP should include both the applicable time in the UK at the time (GMT or BST) and, if different, the local time in the location where the CTP operational incident was detected.

Intermediate Incident Report

8.21 A CTP must, as soon as is practicable after any significant change in circumstances from that described in the initial incident reports, and any intermediate incident reports it may have previously submitted, if applicable (including the CTP operational incident being resolved) and in so far as it is aware at the relevant time, provide the regulators and the affected firms with an intermediate incident report containing the information in Table 5.

Table 5: Information in a CTP's intermediate incident report(s)

Information that must be provided to the regulators and affected firms
(1) any information that the CTP reasonably considers will assists the regulators and affected firms in understanding the nature and extent of the CTP operational incident; (2) steps taken to resolve the CTP operational incident; (3) if the CTP operational incident has been resolved, the time and date that the CTP operational incident was resolved; and (4) any other information which the CTP reasonably considers to be relevant to the regulators and affected firms.

8.22 Examples of a significant change triggering a requirement to submit an intermediate incident report include but are not necessarily limited to:

- the CTP resolving the incident;
- the CTP identifying the root cause of the incident;
- the impact of an incident becoming more severe. For instance, if the appropriate maximum tolerable level of disruption for the systemic third party service(s) affected is breached (and hadn't been breached at the time of initial incident report);
- adverse coverage in mainstream or social media, disinformation or misinformation;
- the incident triggering or incentivising other incidents eg cyber-criminals exploiting a CTP operational incident to distribute malware disguised as fixes or updates linked to that incident;
- the CTP operational incident triggering the threshold for notifying or reporting another regulator (besides those mentioned in the initial incident notification); and
- the activation or escalation of the CTP's incident management measures (as described in section 7).

8.23 If the only significant change since the initial incident report is that the CTP resolves the incident, the intermediate incident report can be limited to a notification that the incident has been resolved. If, in the process of resolving the incident, the CTP comes across other information listed in Table 5 (eg discovering the root cause of the incident), it should mention it in its intermediate incident report that the incident has been resolved.

8.24 An example of the type of information that may assist the regulators and affected firms in understanding the nature and extent of the CTP operational incident includes (but is not limited to), in relation to cyber-attacks:

- the type of threat actor (including known capabilities and motives);
- the complexity and novelty of the attack; and
- whether the attack involved the exploitation of vulnerabilities listed in a public Common Vulnerabilities and Exposures database[40].

8.25 An example of actions taken to resolve the CTP operational incident or mitigate its impact include, but is not limited to, steps taken by the CTP to address misinformation and disinformation relating to the CTP operational incident in the mainstream or social media.

8.26 The frequency, level of detail and timing of submission of intermediate incident reports should balance the competing needs of the:

- CTP to prioritise the resolution the incident; and
- regulators and affected firms to be updated on the evolution of the incident.

[40] https://cve.mitre.org/

8.27 The regulators may ask a CTP to provide intermediate reports and other information relating to a live CTP operational incident at a time or frequency specified by them (and, if appropriate direct it to do so under s312N of FSMA).

8.28 As with initial reports, a CTP can:

- leverage updates to other customers or authorities to comply with the requirement to provide intermediate incident reports, as long as these include the information required by the regulators' rules; or
- use the voluntary template, when available.

Final incident report

8.29 A CTP must, within a reasonable time of the CTP operational incident being resolved, provide the regulators and the affected firms with the information in Table 6:

Table 6: Information in a CTP's final incident report

Information that must be provided to the regulators and affected firms
(1) the time and date that the CTP operational incident was resolved; (2) a description of the root causes (in so far as it is aware at the time of submission); (3) a description of any remedial actions the CTP has or is planning to put in place and an estimated timeline for the completion of those remedial actions; (4) a description of the CTP's assessment of: - the likelihood of recurrence of the CTP operational incident; and - the long-term implications of the CTP operational incident; (5) a description of identified areas for improvement for the CTP and, where relevant, the affected firms; (6) any other information the CTP reasonably considers to be relevant to affected firms; and (7) to the regulators only, any other information the CTP reasonably considers to be relevant to the regulators.

8.30 A clear, thorough final report is key to ensuring that CTPs, affected firms and the regulators identify and implement lessons learnt from a CTP operational incident.

8.31 The regulators normally expect a CTP to submit a final incident report within 30 working days of the resolution of the incident. However, a longer timeframe may be appropriate if, for instance, the root cause of the incident is unclear, or the CTP needs longer to identify lessons learnt and develop a remediation plan. Where a CTP envisages needing longer than 30 working days to submit its final incident report, it

should inform the regulators of its intended date for submitting this report. This intended date should consider CTP Fundamental Rule 6 and be provided within a reasonable timeframe based on the circumstances of the CTP operational incident. The regulators may ask a CTP to provide its final incident report on a specific date or timeframe (and, if appropriate direct it to do so under s312N of FSMA).

8.32 The information that a CTP should include in its final incident report relating to areas for improvement for affected firms should consist of general guidance applicable, and of potential value to, all affected firms. For instance, suggested actions (eg installation of a specific software patch) to ensure that affected firms recover fully from the CTP operational incident, and to prevent the incident from reoccurring. The description of identified areas for improvement for the CTP should be comprehensive and cover any areas for improvement in the CTP's operations identified in connection with the incident. For instance, if a CTP suffers an insider attack from an employee, the identified areas for improvement in its final incident report should identify areas for improvement in its pre-employment screening, ongoing monitoring and other processes (and proposed remediation).

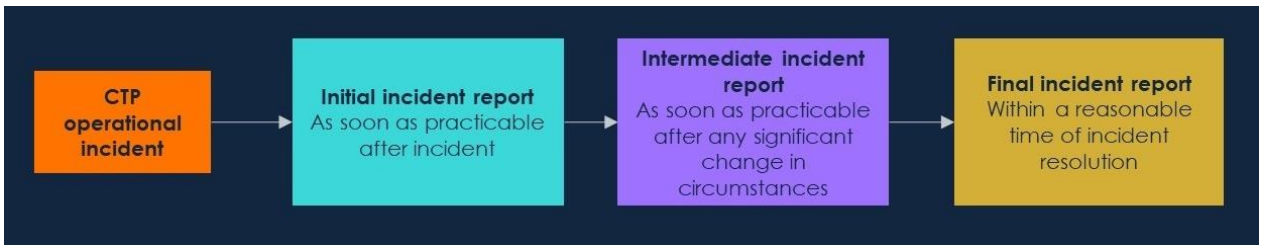


Figure 2: Phased approach to incident reporting

Notifications

8.33 In addition to the incident reporting requirements examined above, a CTP must notify the regulators immediately where there is an actual or potential circumstance or event that seriously and adversely impacts or could seriously and adversely impact the CTP's ability to deliver any of its systemic third party services or meet any of its obligations under the regulators' rules, including where:

- civil proceedings are brought by or against the CTP or a claim or dispute is referred to alternative dispute resolution in any jurisdiction;
- disciplinary measures or sanctions have been imposed on the CTP by any statutory or regulatory authority in any jurisdiction (other than the regulators), or the CTP becomes aware that one of those bodies has commenced an investigation into its affairs;
- the CTP is in financial difficulty and is considering entering into an insolvency proceeding or a restructuring plan in any jurisdiction, or any such proceedings are likely to be brought against it in any jurisdiction; and

- the CTP is subject to criminal proceedings, or has been prosecuted for, or has been convicted of, a criminal offence in any jurisdiction involving fraud or dishonesty.

8.34 Unlike for reports of CTP operational incidents there is no mandatory information that CTPs must or should include in these notifications, nor is there a template (mandatory or voluntary).

Inaccurate, false, or misleading information

8.35 A CTP must take reasonable steps to ensure that all information it gives to the regulators and firms in accordance with the CTP duties (including information required the incident reporting, and notification rules) is:

- factually accurate or, in the case of estimates and judgements, fairly and properly based after appropriate enquiries have been made by the CTP; and
- complete, in that it should include anything of which the regulators would reasonably expect notice (see section 5 for guidance on matter of which the regulators would reasonably expect notice).

8.36 If a CTP is unable to obtain the information required, then it must inform the regulators that the scope of the information provided is, or may be, limited.

8.37 If a CTP becomes aware, or has information that reasonably suggests, that it has or may have provided the regulators with information which was or may have been false, misleading, incomplete or inaccurate, or has or may have changed in a material way, it must notify the regulators immediately. The notification must include:

- details of the information that is or may be false, misleading, incomplete or inaccurate, or has or may have changed – where the changes relate to a CTP operational incident, this can be done in the intermediate notifications discussed above;
- an explanation why such information was or may have been provided; and
- the correct information.

8.38 If the correct information above cannot be submitted with the notification (because it is not immediately available), it must instead be submitted as soon as practicable afterwards.

Electronic submission of information

8.39 As noted in the regulators' rules, CTPs must submit all notifications by electronic means. If electronic means are not available, CTPs should use other appropriate, available means.

9: Public references to a CTP's designated status

Public references to a CTPs' designated status

9.1 HM Treasury designates CTPs by regulations (s312L(1) of FSMA), which will be publicly available.

9.2 A CTP must ensure that it does not, and must take reasonable steps to ensure that any person acting on its behalf does not, in any way indicate or imply that the CTP has the regulators' approval or endorsement by virtue of:

- its designation as a CTP; or
- being overseen by the regulators in respect of services it provides to firms.

9.3 Likewise, a CTP must not, and must take reasonable steps to ensure that any person acting on its behalf does not, in any communication (eg in its marketing material) indicate or imply that the CTP's designation by HM Treasury or oversight by the regulators confers any advantage to a firm or anyone else in using its services as compared to a service provider who is not designated as a CTP.

9.4 The restrictions above do not prevent a CTP from making statements that explain, in a way that is fair, clear and not misleading:

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

9.5 The relevant rules are located in:

- the 'Referring to oversight by the regulators or Treasury designation' chapters of the Critical third parties Parts of the PRA Rulebook, and Bank of England FMI Rulebook; and

- chapter 14 of the Critical third parties sourcebook in the FCA Handbook.

10: Address for service in the UK

10.1 A CTP must provide the regulators with an address in the UK for the service of documents (including 'relevant documents' as defined in **The Financial Services and Markets Act 2000 (Service of Notices) Regulations 2001**[41]). A CTP must also notify the regulators of any change to this information as soon as is practicable.

10.2 These requirements apply to all CTPs. As explained in section 4, a CTP is not required to set up a UK branch or subsidiary as a result of being designated by HM Treasury if they did not have one prior to designation. The requirement to provide the regulators with an address in the UK for the service of documents ensures that the regulators can provide documents such as statutory notices to all CTPs.

10.3 The requirement for an address for service applies in addition to the requirement for CTPs to appoint one or more persons as the designated point of contact for the regulators under Requirement 1 of the CTP Operational Risk and Resilience Requirements. The designated point of contact need not be based at the CTP's UK address for service.

10.4 The relevant rules are located in:

- chapter 11 of the Critical third parties sourcebook in the FCA Handbook; and
- The Address for Service chapters of the Critical third parties Parts of the PRA and Bank of England FMI Rulebooks.

11: Record keeping

11.1 CTP must arrange for orderly records to be kept of its business and internal organisation, in so far as it concerns the provision of services to firms. These records must be sufficient to enable each regulator to:

- perform its oversight functions; and
- ascertain whether or not the CTP has complied with its duties.

The relevant rules are located in:

41 **https://www.legislation.gov.uk/uksi/2001/1420/contents/made**.

- the Record Keeping chapters of the Critical third parties Parts of the PRA Rulebook, and Bank of England FMI Rulebook; and

- chapter 15 of the Critical third parties sourcebook in the FCA Handbook.

12: Transitional arrangements

12.1 The regulators' rules come into force on 1 January 2025. The statutory obligations of a CTP under FSMA and the requirements in the regulators' rules apply to a CTP from the date on which designation takes effect, which will be specified by HM Treasury in the designation order.

12.2 The following requirements for a CTP in the regulators' rules are subject to transitional arrangements:

- to submit its initial self-assessment to the regulators, which it must do within three months of the date on which designation takes effect (see section 7);

- to have completed its initial mapping within twelve months of the date specified by HM Treasury in the designation order (see Requirement 6 in section 6);

- to carry out its first round of scenario testing, which the CTP should do within twelve months of the date specified by HM Treasury in the designation order. This includes amending or enhancing existing scenario-testing programmes to meet the regulators requirements;

- to maintain and operate an incident management playbook within twelve months of the date specified by HM Treasury in the designation order. This includes updating and enhancing the CTP's existing incident management playbook where applicable; and

- to carry out its first incident management playbook exercise, which it must do no later than 12 months from the date specified by HM Treasury in the designation order.

12.3 Although the requirements in the regulators' rules apply directly to CTPs they may, in practice, require amendments to their contractual arrangements with firms, and their Key Nth Party Providers. Where this is the case, CTPs should seek to review and update contractual agreements entered into before their designation at the first appropriate contractual renewal or revision point following their designation.