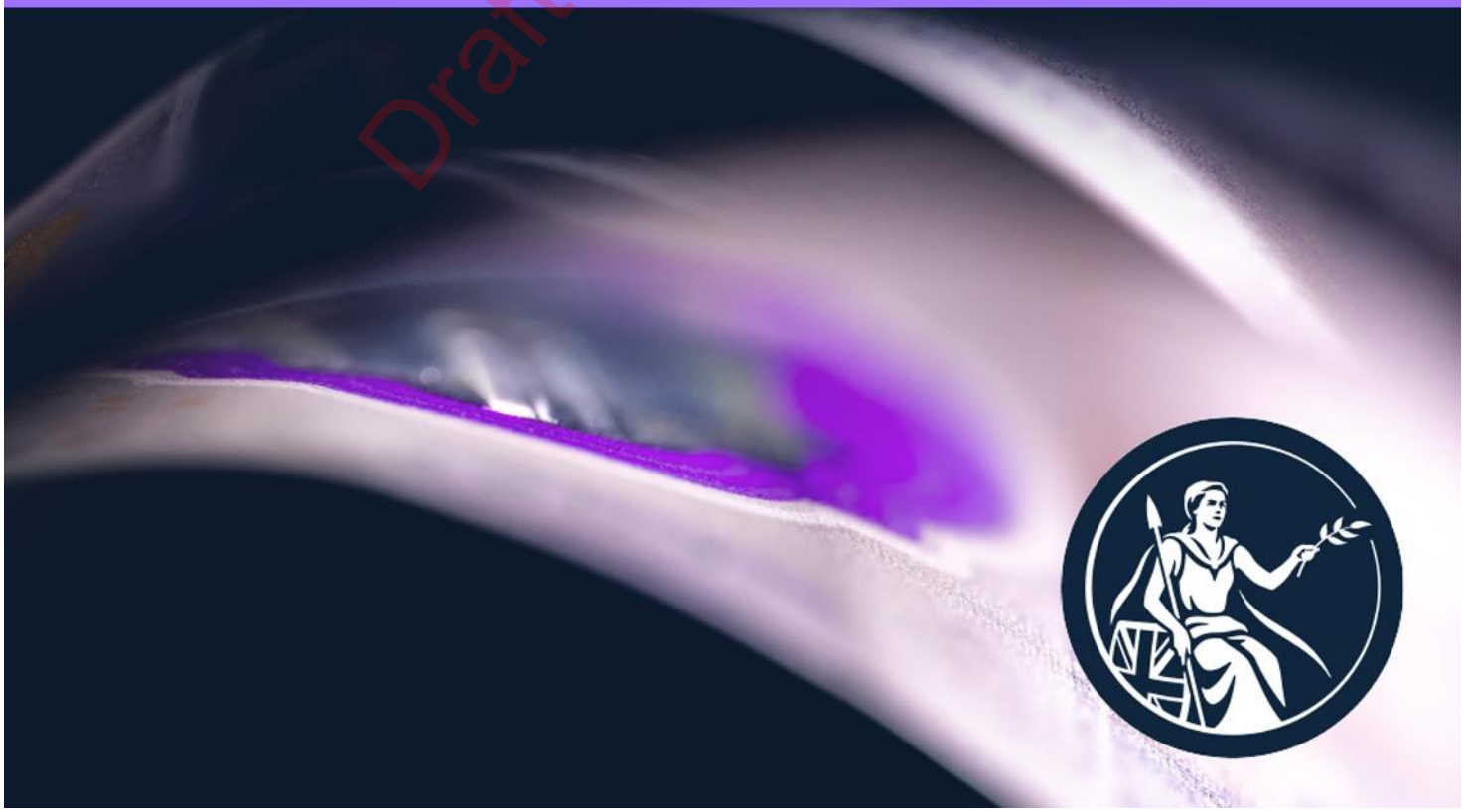
Bank of England PRA

FCA FINANCIAL CONDUCT AUTHORITY

Appendix 4 to CP26/23 – Operational resilience: Critical third parties to the UK financial sector

Supervisory statement

December 2023



Bank of England | Prudential Regulation Authority | Financial Conduct Authority

Operational resilience: Critical third parties to the UK financial sector

Supervisory statement

December 2023

Prudential Regulation Authority | 20 Moorgate | London EC2R 6DA

Contents

1: Introduction

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

1.2 This supervisory statement sets out the regulators' expectations of how critical third parties (CTPs) should comply with and interpret the requirements in the regulators' rules. These requirements seek to manage potential risks to the stability of, or confidence in, the UK financial system that may arise as due to a failure in, or disruption to the services that CTPs provide to firms and financial market infrastructure entities (FMIs).

Structure of this supervisory statement

- Chapter 2 – sets out the key terms used in this supervisory statement.
- Chapter 3 – provides an overview of the oversight regime for CTPs.
- Chapters 4 – sets out how a CTP should comply with the requirements in the CTP Fundamental Rules;
- Chapter 5 – sets put how a CTP should comply with the Operational Risk and Resilience Requirements.
- Chapter 6 – sets out how a CTP should comply with the requirements on information-gathering and testing.
- Chapter 7 – sets out how a CTP should comply with the notification requirements.
- Chapter 8 – sets out how a CTP should comply with the requirements on public references to their designation.
- Chapter 9 – sets out how CTPs whose head offices are outside the UK should comply with the requirement to appoint a UK representative.
- Chapter 10 – sets out how CTPs should comply with the requirements on record-keeping.

2: Key terms

2.1 The regulators consider it important to define key terms to ensure a clear and consistent understanding by CTPs of the regulators' requirements in their rules and the accompanying expectations in this supervisory statement. The 'key entities and persons' and 'key concepts' defined in this section should be read alongside the relevant definitions in the regulators' rules and the Financial Services and Markets Act (2000) (FSMA) as amended by the **Financial Services and Markets Act 2023** (FSMA 2023).[1]

Key entities and persons

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

- A **firm** is:

(i) any person 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 s31 FSMA);

(ii) a relevant service provider, as defined in s312L(8) FSMA, which encompasses:

- an authorised payment institution, small payment institution, or registered account information services provider, as defined by regulation 2(1) of the **Payment Services Regulations 2017**;[2] or
- an electronic money institution, as defined in regulation 2(1) of the **Electronic Money Regulations 2011**;[3] or

- A **Financial Market Infrastructure entity** (FMI) is an entity defined in s312L(8) FSMA, including a:
  (i) recognised clearing house, including a central clearing counterparty (CCP);
  (ii) recognised central securities depository (CSD);
  (iii) UK recognised investment exchange (RIE);
  (iv) recognised payment systems (RPS); and
  (v) specified service provider (SSP) to a RPS.

- An **employee** is an individual who is employed or appointed by a CTP in connection with its business, whether under a contract of service or for services or otherwise; or whose services, under an arrangement between that CTP and a third party, are placed at the disposal and under the control of the CTP.

1 **www.legislation.gov.uk/ukpga/2023/29/contents/enacted**.
2 **www.legislation.gov.uk/uksi/2017/752/contents/made**.
3 **www.legislation.gov.uk/uksi/2011/99/contents/made**.

- A CTP's **supply chain** is the network of persons that provide infrastructure, goods or services and other inputs directly or indirectly utilised by a CTP to deliver, support, and maintain a material service.

- A **Person Connected with a CTP** is defined in s312P(10) FSMA, and may include:
  (i) members of the CTP's group;
  (ii) the controller(s) of the CTP ie a person who holds influence over a CTP directly or indirectly through ownership rights (see s422 FSMA);[4] or
  (iii) legal and natural person mentioned in Part 1 of **Sch. 15 FSMA**[5] eg an officer or manager of a CTP's parent undertaking.

The term Person Connected with a CTP includes legal or natural persons who come under the definition in s312P(10) FSMA at any time from the date when the CTP is designated, but subsequently cease to do so.

- A **key Nth party service provider** is an entity or person that is part of a CTP's supply chain and is essential to its ultimate delivery of a material service to firms or FMIs.

- A **skilled person** is a person appointed to:
  (i) make and deliver to the regulators a report under s166 FSMA; or
  (ii) collect or update information as required by the regulators under s166A FSMA.

- **Financial sector incident response frameworks** is an umbrella term for any arrangements and frameworks put in place by firms, FMIs, authorities, or other persons for coordinating responses to incidents affecting the delivery of a material service.

Key concepts

- **Oversight Functions** is as an umbrella term for all the regulators' functions in relation to a CTP conferred by or under FSMA, including their statutory powers to:
  (i) make rules imposing duties on a CTP in connection with the provision of services to firms and FMIs (rulemaking powers) (s312M FSMA), and to oversee compliance with any rules made pursuant to this power.
  (ii) direct a CTP in writing to:
    a. do anything; or
    b. refrain from doing anything specified in the direction (s312N-312O FSMA) (powers of direction and procedure).
  (iii) gather information from a CTP and Persons Connected to a CTP, and carry out investigations (s312P FSMA) (information-gathering and investigations powers).

4 **www.legislation.gov.uk/ukpga/2000/8/section/422**.
5 **www.legislation.gov.uk/ukpga/2000/8/schedule/15**.

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

- **CTP duties** means the duties and obligations placed upon a CTP conferred by or under FSMA and the regulators' rules.

- **Material service** is a service (wherever carried out) provided by a CTP to one or more firms a failure in, or disruption to, the provision of which (either individually or, where more than one service is provided, taken together) could threaten the stability of, or confidence in, the UK financial system.

- **Asset** includes data, people, information, and infrastructure.

- **Disruption** includes (in relation to a service) complete or partial failure of that service or a significant degradation to the quality of that service.

- **Relevant incident** is either a single event or a series of linked events that actually or has the potential to:
  (i) seriously disrupt the delivery of a material service; or
  (ii) seriously and adversely impact the availability, authenticity, integrity, or confidentiality of assets relating or belonging to the firms which the CTP has access to as a result of it providing services to firms or the potential to result in a serious loss of such assets.

- A **Financial Sector Incident Management Playbook** is a document setting out how a CTP will communicate with and support the regulators, and the firms and FMIs it provides services to (individually and collectively) in respect of incidents that affect the delivery of a material service.
- In the regulators' rules and/or this supervisory statement, the following terms have the definition in the Financial Stability Board (FSB) Cyber Lexicon:[6]
  (i) Cyber incident response plans
  (ii) Cyber Resilience
  (iii) Cyber Risk
  (iv) Cyber Security
  (v) Insider Threat
  (vi) Penetration Testing
  (vii) Situational Awareness
  (viii) Threat Actor
  (ix) Vulnerability Assessment
  (x) Zero-Day vulnerability.

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

2.2 In this supervisory statement:

- 'must' describes a requirement on CTPs in FSMA and/or the regulators' rules; and
- 'should' sets out how the regulators expect CTPs to comply with a requirement. These expectations are outcomes-focused and recognise that there may be a number of valid ways to meet a requirement.

3: Overview of the oversight regime for CTPs

Overall objective

3.1 The overall objective of the oversight regime for CTPs is to manage potential risks to the stability of, or confidence in, the UK financial system that may arise due to a failure in, or disruption to, the services that a CTP provides to firms and FMIs (either individually or, where more than one service is provided, taken together). The oversight regime for CTPs seeks to achieve this overall objective by improving and overseeing the resilience of these services. CTPs should approach the requirements in FSMA and the regulators' rules, and the accompanying expectations in this supervisory statement with this overall objective in mind.

3.2 Consistent with this overall objective, it is vital that CTPs acknowledge and understand the potential systemic risk that failure in, or disruption to, their services to firms and FMIs (in particular their material services) could cause. A key goal of the requirements in FSMA and the regulators' rules, and the accompanying expectation in this supervisory statement is to ensure CTPs deliver a level of resilience commensurate with the significant impact that a disruption of their services could cause to the UK financial sector, and that they respond appropriately to incidents affecting the services they provide.

3.3 For the purposes of the oversight regime for CTPs, the terms 'service' and 'failure' have their ordinary English language dictionary meaning, and should be interpreted broadly and purposefully in light of the regime's overall objective. A CTP's services to firms and FMIs may include but are not limited to:

- a facility, as provided in s312L(8) FSMA;
- activities, functions, processes and tasks, as noted in the Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities - Consultative document (FSB TPR toolkit);[7] and
- Information and Communications Technology (ICT) Services as defined in Article 3(21) of the European Union (EU) Digital Operational Resilience Act (DORA).[8]

3.4 The term 'disruption' is defined in the regulators' rules and section 2, and should be interpreted as including any event or series of linked events that:

7 www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities.
8 EUR-Lex - 32022R2554 - EN - EUR-Lex.

- causes a loss or significant degradation to the quality, confidence in or functionality of one or more services that a CTP provides to firms and/or FMIs requiring immediate or urgent attention. This may include, but is not limited to:
  - a complete or partial failure of the services;
  - the services becoming unavailable for an extended period; and/or
  - the services not performing as intended.
- adversely affects the authenticity, availability, confidentiality, or integrity of any assets (including data), belonging to firms and FMIs or relating to the services that the CTP provides to those firms and FMIs.

Focus on CTPs' services to firms and FMIs

3.5 Although HMT will designate CTPs at the entity level, the oversight regime for CTPs only applies to the services that CTPs provide to firms and FMIs.

3.6 The CTP Fundamental Rules in section 4 apply to all of the services that a CTP provides to firms and FMIs. Other (more granular) requirements only apply to a CTP's material services. For instance, the Operational Risk and Resilience Requirements in section 5, the scenario testing requirements in section 6 and the incident notification requirements in section 7.

3.7 Material services are defined as those services whose failure or disruption could threaten the stability of, or confidence in, the UK financial system. They are also the services that HMT must have regard to when designating a CTP.

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

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

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

- recommend to HM Treasury that it removes the designation of any CTP which they consider no longer meets the statutory test for designation; and

- for those CTPs who continue to meet the criteria for legislation, flag whether the review has highlighted any potential changes to their list of material services. For instance, potential new material services, or formerly material services which may potentially no longer be material. The regulators will use this analysis to facilitate a dialogue with CTPs about possible changes to their list of material services.

3.11 Although the regulators' primary focus is on material services, they may also look at any non-material services that a CTP provides to firms and FMIs if appropriate to advance their objectives.

3.12 Consistent with the regulators' focus on a CTP's services to firms and FMIs, there is no requirement for a CTP whose head office is outside the UK to establish a UK subsidiary under the oversight regime. However, certain requirements in the regulators' rules ensure that:

- there is a central point of contact for the regulators at each CTP (see section 4); and
- a CTP whose head office is outside the UK nominates a legal person to perform certain functions on their behalf, such as receiving statutory notices issued by the regulators under FSMA (see section 9).

Interaction with the requirements for firms and FMIs

3.13 The oversight regime for CTPs complements the requirements and expectations for firms and FMIs, in particular on operational resilience and outsourcing, and third party risk management. The CTP oversight regime sits alongside these requirements and expectations but does not blur, eliminate, or reduce the accountability of firms, FMIs, their boards and senior management (including individuals performing Senior Management Functions (SMFs)).

Alignment to international standards

3.14 The oversight regime for CTPs draws inspiration from global standards. In particular:

- the FSB:
  - Cyber Lexicon;
  - FSB TPR toolkit;
  - Effective Practices for Cyber Incident Response and Recovery;[9] and
  - Recommendations to Achieve Greater Convergence in Cyber Incident Reporting (FSB CIR Recommendations).[10]

9 **FSB Effective Practices for Cyber Incident Response and Recovery: Final Report.**

10 **FSB Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report.**

- the Basel Committee on Banking Supervision (BCBS):
  - Principles for Operational Resilience;[11]
  - Revised Principles for the Sound Management of Operational Risk (PSMORs) ;[12] and
  - High-level principles for business continuity.[13]
- 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' in Annex F;[14] and
  - PFMIs: Assessment methodology for the oversight expectations applicable to critical service providers.[15]

3.15 The UK oversight regime for CTPs is designed to be interoperable with other regimes aimed at managing systemic risks posed by what the FSB TPR toolkit refers to as 'systemic third party dependencies' and 'financial sector critical service providers'.[16] These regimes include DORA in the EU and the Bank Service Company Act in the US. To promote interoperability with these regimes, the regulators may:

- ask CTPs for information provided to the authorities responsible for these regimes, and take it into consideration in their oversight (see section 5);
- accept incident notifications or reports submitted by CTPs to firms, FMIs, and/or the authorities responsible for these regimes, as long as they include the information specified in the regulators' rules and section 6; and
- subject to appropriate cooperation and information-sharing arrangements, exchange information relating to CTPs of mutual interest with the relevant authorities.

11 **BCBS Principles for operational resilience.**

12 **BCBS Revisions to the Principles for the Sound Management of Operational Risk.**

13 **BCBS High-level principles for business continuity.**

14 **CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI).**

15 **CPMI-IOSCO Principles for financial market infrastructures: Assessment methodology for the oversight expectations applicable to critical service providers.**

16 A service provider to financial institutions whose services have been deemed by financial authorities to give rise to a systemic third-party dependency with potential implications on financial stability, including potential systemic risk case of disruption or failure. This is a general concept, and the specific term and definition may differ depending on jurisdictions.

Proportionality

3.16 All CTPs, will by definition, have been assessed as providing services for which failure in, or disruption to, the provision of these services could threaten the stability of, or confidence in, the UK financial system. All CTPs are therefore subject to consistent, minimum requirements, expectations, and oversight. However, when overseeing CTPs, the regulators will take a proportionate approach.

3.17 If a CTP provides services to multiple sectors or in multiple jurisdictions, it may be able to rely on its existing processes if it can demonstrate to the regulators that these processes meet the requirements in the regulators' rules and the accompanying expectations in this supervisory statement.

Format of the regulators' rules for CTPs

3.18 Each regulator has a standalone statutory rulemaking power over CTPs. However, the Regulators have a statutory duty to coordinate the exercise of their functions over CTPs (s312U FSMA), including when making rules for CTPs.

3.19 As a result, the requirements for CTPs are set out in three separate but substantively identical rule instruments.[17]

3.20 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 drafting style of the regulators and the format of their respective handbooks and rulebooks.

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

[17] 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 rulebook (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.

Supervisory Statements and Statements of Policy on CTPs

3.22 This joint Bank/PRA and FCA supervisory statement should be the key source of guidance for CTPs on how to approach, comply with, and interpret the requirements in the regulators' rules. In the event of any perceived inconsistencies, the text of the rules take precedence.

3.23 The regulators will also issue the following documents in due course.

- Statements of policy (SoP) on their approach to enforcement over CTPs
  - The Bank of England's approach to enforcement: statements of policy and procedure;[18] and
  - FCA: Statement of policy on the use of disciplinary powers over CTPs.
- Guidance on the regulators' use of skilled person reviews on CTPs:
  - Bank/PRA SSX/24 Reports by skilled persons: Critical Third Parties; and
  - Chapter 11 and 12 of the Critical Third Parties Sourcebook in the FCA Handbook.

Transitional arrangements

3.24 The statutory obligations of a CTP under FSMA and the majority of the requirements in the regulators' rules apply from the point it is designated by HMT.

3.25 However, certain requirements are subject to transitional arrangements. In particular:

- the requirement on CTPs to submit a self-assessment to the regulators (which they must do within three months of designation and thereafter within twelve months of the last submission (see section 6); and

- The requirements on CTPs to produce a map (see Section 5), and produce and test their financial sector incident management playbook (see Section 6), which they must do within 12 months of designation and annually thereafter.

3.26 During this transitional twelve month period, the regulators may engage with CTPs to check on progress towards compliance with these requirements and, if appropriate, request drafts of their maps or financial sector incident management playbooks.

18 Consultation paper 9/23 – **The Bank of England's approach to enforcement: proposed changes and clarifications.**

4: CTP Fundamental Rules

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

- Critical Third Parties Fundamental Rules chapter 3 of the Critical Third Parties (CTPS) sourcebook in the FCA Handbook of the Critical Third Parties Sourcebook in the FCA Handbook; and
- the Critical Third Parties Fundamental Rules (Chapter 3) in the Critical Third Parties Part of the PRA and Bank Rulebooks.

BOX 1: CRITICAL THIRD PARTY FUNDAMENTAL RULES

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

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

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

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

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

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

4.2 The CTP Fundamental Rules are high level rules that collectively act as an expression of the regulators' overall objective (see section 3). They provide a general statement of a CTP's fundamental obligations under the oversight regime.

4.3 The CTP Fundamental Rules apply to all the services that a CTP provides to firms and FMIs (wherever carried out). A CTP should interpret phrases such as 'conduct their business', 'organise and control their affairs' etc accordingly.

5: CTP Operational Risk and Resilience Requirements

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

- Chapter 4 of the Critical Third Parties sourcebook in the FCA Handbook; and
- the 'Critical Third Party Operational Risk and Resilience Requirements' (Chapter 4) in the Critical Third Parties Parts of the PRA and Bank Rulebooks.

5.2 As noted in section 3, the CTP Operational Risk and Resilience Requirements only apply to a CTP's material services.

5.3 A CTP must have in place sound, effective and comprehensive strategies, controls, processes, and systems that enable it to adequately meet the Operational Risk and Resilience Requirements.

5.4 A CTP's compliance with the Operational Risk and Resilience Requirements, and the resilience of its material services should evolve and improve as it learns from incidents and testing (including but not limited to testing required by the regulators' rules). The objective to constantly learn and evolve pervades the Operational Risk and Resilience Requirements.

Requirement 1: governance

5.5 A CTP must ensure that its governance arrangements promote the resilience of each of its material services, including by:

- appointing a natural person who:
  - is a CTP employee, or a member of its governing body; and
  - has appropriate authority, knowledge, skills and experience to act as the central point of contact with the regulators in their capacity as authorities having oversight functions;
- establishing clear roles and responsibilities at all levels of its staff involved in the delivery of any material services, with clear and well-understood channels for communicating and escalating issues and risks;

- establishing, overseeing, and implementing an approach that covers the CTP's ability to:
    - prevent, respond and adapt to, as well as recover from any event that causes disruption to the delivery of a material service;
    - learn from those events and any testing undertaken; and
- ensuring appropriate review and approval of any information provided to the regulators.

Appointment of a central point of contact for the regulators

5.6. A CTP may appoint more than one individual to act as the central point of contact but should ensure that their respective responsibilities are clear (especially if they are split), and that they have up to date knowledge, skills and experience of the:

- type of services that the CTP provides to firms and FMIs; and
- requirements and expectations applicable to the CTP, and the firms and FMIs it provides services to eg on operational resilience.

5.7 A CTP must notify the regulators in writing of the name, business address, email addresses, telephone numbers, and out of hours contact details of the appointed person and update the regulators of any changes. Updates should be notified to the regulators as soon as reasonably practicable.

5.8 The appointed employee(s) or member(s) of the governing body should be contactable during UK business hours regardless of whether they are located in the UK or not.

5.9 The regulators will usually engage with a CTP via its appointed employee(s) or member(s) of its governing body. However, if appropriate, the regulators may also engage with other CTP employees or members of its governing body, such as specialists in a specific area.

Appropriate review and approval of information provided to the regulators

5.10 A CTP must ensure that any information it provides to the regulators undergoes appropriate review and approval.

5.11 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 the CTP's annual self-assessment should be approved and reviewed by the top layer of decision-making responsible for the delivery of material

services to firms and FMIs (see section 6). This layer could be the CTP's governing body (or a committee thereof), senior management, or a dedicated committee, individual, or group.

5.12 In line with CTP Fundamental Rule 6, a CTP should ensure, as part of this review and approval process, that any information it provides to the regulators is (to the best of its knowledge) accurate, complete, and includes anything of which the regulators would reasonably expect notice.

Requirement 2: risk management

5.13 A CTP must effectively manage risks to its ability to continue to deliver a material service including by:

- identifying and monitoring relevant external and internal risks;
- ensuring that it has risk-management processes that are effective at managing those risks; and
- regularly updating its risk management processes to reflect issues arising and lessons learned from:
  - a disruption to a material service;
  - engagement with regulators;
  - new and emerging risks; and
  - any associated testing, including but not limited to testing carried out in accordance with sections 5 and 6.

5.14 Many of the risks to a CTP's delivery of material services are likely to be operational. Examples include but are not limited to:

- dependency and supply chain risks (see Requirement 3);
- cyber and technology risks (see Requirement 4);
- change management risks (see Requirement 5);
- data risks;
- insider threats eg conduct risks from current and former employees;
- model risks; and

- risks to the CTP's physical assets eg as a result of climate change.

5.15 A CTP should also consider financial risks that may affect its ability to deliver material services, in particular, risks to its financial viability. These financial risks could be internal eg high leverage, or external eg market volatility or a deterioration in the economic environment. In both cases, the CTP should have in place appropriate transitional measures to respond to an unexpected termination of any of its material services, including in case of insolvency (see Requirement 8). On a risk-based approach, the regulators may ask a CTP for evidence of its ongoing financial viability and its management of financial risks.

5.16 A CTP should have a sound risk management framework to manage risks to its delivery of material services. This framework should include:

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

5.17 A CTP should monitor risks on an ongoing basis, including through horizon scanning, testing, and the use of threat intelligence.

5.18 Although a CTP should manage all relevant types of risk as part of its risk management processes under Requirement 2, there are three specific risks that are considered individually in Requirements 3 to 5 given their importance and relevance to the oversight regime for CTPs. These risks include:

- dependency and supply chain risk management;
- cyber and technology risks; and
- change management risks.

Requirement 3: dependency and supply chain risk management

5.19 A CTP must identify and manage risks to its supply chain that could affect its ability to deliver a material service, including due to dependencies on:

- a Person Connected with the CTP; and
- Key Nth party service providers.

5.20 In particular, a CTP must take all reasonable steps to ensure that each person in its supply chain:

- understands the requirements that apply to the CTP by virtue of the 'CTP duties' (which is an umbrella term in the regulators' rules covering all requirements for CTPs under FSMA and the rules);
- acts to facilitate the CTP meeting those requirements; and
- provides the regulators with access to information relevant to the regulators' exercise of their oversight functions.

5.21 A CTP's compliance with Requirement 3 should form part of its wider risk management processes under Requirement 2 and be in line with CTP Fundamental Rule 4. In line with the principle of proportionality (and consistent with the FSB TPR toolkit), when managing dependency and supply chain risks CTPs should focus on Key Nth party service providers (as defined in section 2) and other parts of their supply chain that are knowingly essential to the delivery of material services to firms and FMIs, or which have access to confidential or sensitive data belonging to the firms and FMIs.

5.22 A CTP should:

- perform appropriate due diligence before entering into sub-contracting arrangements that are key to its delivery of material services and monitor these arrangements on an ongoing, or regular (at least annual) basis thereafter;
- be transparent with the regulators (in line with CTP Fundamental Rule 6) and the firms and FMIs it provides services to about which parts of its supply chain are essential to its delivery of material services;
- obtain information about incidents in its supply chain that may affect its delivery of material services – a CTP should also ensure that there are no impediments (eg contractual restrictions) on its ability to share the relevant information with the regulators and the firms and FMIs it provides services to (see Section 7);
- include scenarios involving supply chain disruption in its testing (see Section 6); and

- incorporates lessons learned from (i) disruption to; and (ii) testing of its supply chain into its risk management and incident management processes (see Requirements 3 and 7).

Requirement 4: Technology and cyber resilience

5.23 Under Requirement 4, a CTP must ensure the resilience of any technology that delivers, maintains or supports a *material service*, including by having:

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

5.24 All Operational Risk and Operational Resilience Requirements are relevant to a CTP's cyber and technology risk management. However, cyber and technology risks have unique characteristics that warrant individual consideration. In particular, the:

- complexity of technology infrastructure and its design can make it difficult to monitor and manage in line with business expectations;
- presence of active, persistent, and sophisticated threat actors, which can make it difficult to identify cyber-attacks, assess the damage they cause, or eradicate them fully;
- broad range of entry points through which a CTP may be compromised; and
- potential for cyber-risks to crystalise and propagate stealthily and rapidly, including via the CTP.

5.25 Consequently, in addition to complying with the Operational Risk and Operational Resilience Requirements, a CTP's technology and cyber resilience measures should include but not be limited to:

- a framework that clearly articulates how the CTP determines its technology and cyber resilience objectives, and how it identifies, assesses, mitigates, measures, and manages technology and cyber risks. In addition to technology, this framework should cover the CTP's assets (including data), people and processes;

- measures to protect, detect, respond, and recover critical assets from IT disruptions and cyber-attacks;
- a culture and processes that seek to ensure material services are resilient by design;
- IT controls that minimise the likelihood and impact of IT incidents on material services, and on the resources that support them;
- security controls that minimise the likelihood and impact of a successful cyber-attack on material services, and the resources that support them;
- capabilities to monitor anomalous activity (in real-time, or near-real time); and detect incidents;
- capabilities to identify, assess and promptly remediate vulnerabilities;
- comprehensive, regular testing to validate the effectiveness of its technology and cyber resilience (including, but not limited to tests required by the regulators' rules (see Section 6)); and
- situational awareness underpinned by effective cyber threat intelligence, which should enable a CTP to understand the cyber threat environment in which it operates and the adequacy of its cyber resilience and cyber security measures.

5.26 A CTP should also ensure that cyber and technology response and recovery measures are considered as part of compliance with Requirement 7: incident management.

Requirement 5: change management

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

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

5.28 A CTP's review and approval of changes to its material services should cover the lifecycle of the relevant changes (from inception to termination) and consider:

- inherent and residual risks;
- the need to commit appropriate resources to ensure the resilience and success of the proposed change;
- new processes to be implemented;
- changes to people, including employees, key Nth party service providers and other essential parts of the supply chain;
- changes to the risk profile of existing material services (including risk thresholds or limits);
- the use of appropriate metrics to assess and monitor risks relating to the proposed change;
- agreeing an appropriate timeframe for implementation that does not incentivise excessive risk-taking or rushed decision-making; and
- implementing appropriate controls, risk management processes, and risk mitigation.

5.29 To minimise the risk of a failure or undue disruption, the regulators expect that before commencing a change to a material service, a CTP should plan what it will do if the change fails. This may include but would not be limited to reversing or rolling back the change.

5.30 A CTP should continue monitoring changes to material services for an appropriate period after their implementation to identify and manage any unexpected risks.

Requirement 6: mapping

5.31 Under Requirement 6 a CTP must:

- (subject to the transitional arrangements in Section 3 and the bullet below) identify and document:
    - resources, including the assets, and technology, used to deliver, support, and maintain each material service it provides; and

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

- have completed the identification and documentation of these resources within 12 months of being designated by HMT, and keep it up to date at all times thereafter.

5.32 If two or more material services are supported by the same resources, a CTP may produce a single map but should make clear all the material services it applies to.

5.33 Mapping should:

- enable a CTP to identify vulnerabilities by:
  - distinguishing those resources across the supply chain that are essential to its delivery of material services, and any interconnections between them; and
  - ascertaining whether these resources are fit for purpose.
- facilitate a CTP's scenario testing (see section 6) – a map of the relevant material services is necessary to design a scenario and test it effectively.

5.34 Although there is no prescribed format or template for a CTP's maps, they should:

- focus on the resources that are essential to the CTP's delivery of material services;
- be sufficiently granular to meet the outcomes in para. [5.28]; and
- be updated annually and following certain events, such as a change to a key Nth party service provider.

5.35 Table 1 provides an illustrative, non-exhaustive list of some of the resources that a CTP may include in its maps. However, each CTP is responsible for identifying the resources required for delivering, supporting, and maintaining its material services, including any not listed below. A CTP's map should also identify known vulnerabilities in the supply chain eg concentrations on specific Nth party service providers or geographic regions.

Table 1: illustrative list of resources

Types	Examples
Data and Information	● Customer firms and FMI data. ● Open source data. ● Proprietary data. ● Data analytics tools. ● Service level data.
Facilities	● Jurisdictions/regions where material services are provided. ● Premises used for the delivery of material 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 material services to firms and FMIs, including: (i) key departments and functions at the CTP; (ii) persons connected to the CTP; (iii) key Nth party service providers; and (iv) managed service providers (MSPs) approved by the CTP.
Processes	● Design and approval of material services. ● Assurance (including testing) of material services. ● Change management. ● Incident management plans (see below).
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
Supporting infrastructure	● Cables. ● Cooling. ● Public telecommunications operators. ● Utilities (electricity, water). ● Transport (Air, shipping etc).

Requirement 7: incident management

5.36 A CTP must appropriately manage incidents that adversely affect or may reasonably be expected to adversely affect the delivery of a material service, including by:

- implementing appropriate measures to respond and recover from incidents in a way that minimises their impact;
- setting a maximum tolerable level of disruption to the service;
- maintaining and operating a financial sector incident management playbook; and
- coordinating and engaging with arrangements put in place by firms, FMIs, authorities or other persons for coordinating responses to incidents adversely affecting the UK's financial sector or parts of it. For example, the Sector Response Framework (SRF) owned and maintained by the Cross-Market Operational Resilience Group (CMORG).[19]

5.37 The requirements on incident management are key to ensuring that CTPs have regard to the potential systemic risks posed by disruption to their material services when determining how to respond to an incident.

19 www.cmorg.org.uk.

Response and recovery measures

5.38 To comply with Requirement 7, a CTP should implement response and recovery measures for incidents that affect or may adversely affect its delivery of a material service. A CTP will typically set out these measures in various documents, including:

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

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

- the setting of a maximum tolerable level of disruption for the material service ahead of any incident;
- the classification of incidents based on predefined criteria eg expected recovery time and (if known) their potential impact on the CTP's firm and FMI customers;
- procedures and targets for restoring material services and recovering assets (including data);
- internal and external communication plans; and
- continuous improvement through the incorporation of lessons learned from previous incidents and testing.

5.40 A CTP should use appropriate metrics and targets when setting a maximum tolerable level of disruption for its material services (which may include, but not necessarily be limited to service availability, recovery point objectives (RPOs), recovery time objectives (RTOs) etc). These metrics and targets should:

- take into account and (to the extent possible) be compatible with the impact tolerances that firms and FMIs have set for any important business services that are supported by the material service;
- include at least one time-based metric;

- consider additional, non-time-based metrics if appropriate; and
- cover the delivery of the material service in both business-as-usual circumstances, and times of heightened or peak activity, for instance, if the service fails over to a backup site, different availability zone or region.

5.41 A CTP's incident classification should consider whether the incident warrants immediate and urgent action, including but not limited to specialist teams, senior management, or the CTP's governing body. This may in turn inform whether the incident is a 'relevant incident' which should be notified to the regulators (see section 7).

5.42 A CTP should also:

- Periodically, and at least annually, test and update its response and recovery measures; and
- identify the root causes of incidents, and take all reasonable steps to address them in order to reduce the risk of incidents reoccurring (see Sections 6 and 7).

5.43 A CTP's response and recovery measures should cover incidents with a potential cross-border and cross-sectoral impact.

Financial sector incident management playbook

5.44 The purpose of a financial sector incident management playbook is to mitigate the risks that an incident which adversely affects a CTP's material services (or may reasonably be expected to do so) may pose to the stability of, and confidence in, the financial system. The playbook does this by ensuring that a CTP considers, documents, and regularly tests and reviews how it will communicate with and support the regulators and the firms and FMIs it provides services to (collectively and individually) during these incidents.

5.45 The playbook should set out how the CTP will:

- coordinate its crisis communications with those of the firms and FMIs it provides material services to in order to mitigate risks to the stability of, and confidence in, the financial system –for instance, by collaboratively tackling disinformation and misinformation in the aftermath of an incident; and
- ensure that its firm and FMI customers, and the regulators, receive accurate, consistent, and timely information and support throughout the lifecycle of the incident, including on:
  - the implementation of the CTP's response and recovery measures;
  - any parts of the CTP's supply chain affected by the incident; and
  - other guidance or information that may assist:

- the firms and FMIs that the CTP provides services to in their response and recovery; and
- the regulators in the exercise of their CTP functions.

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

5.47 A CTP may leverage its existing response and recovery measures for the purposes of producing the financial sector incident management playbook.

5.48 A CTP should make its financial sector incident management playbook available to the regulators on request.

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

5.49 A CTP must coordinate and engage with arrangements put in place by firms, authorities, or other persons for coordinating responses to incidents adversely affecting the UK's financial sector or parts of it. The Bank's webpage on Operational resilience of the financial sector[20] mentions some of these frameworks, which include the Sector Response Framework (SRF) or the Financial Sector Cyber Collaboration Centre (FSCCC).

5.50 For the purposes of this requirement, 'engaging' means the CTP ensuring that it has established and rehearsed ways to connect with one or more financial sector incident response frameworks if an incident affecting its material services occurs, so that it can provide appropriate updates and support to the financial sector. Engagement should take place during live incidents but also (as appropriate) in business-as-usual to prepare for potential future incidents. For instance, by establishing and testing appropriate communication channels, processes etc.

5.51 The regulators do not prescribe a specific financial sector incident response framework that CTPs must engage with. Moreover, the frameworks listed on the Bank's webpage are non-exhaustive. Additional frameworks may be created in the future. Given the potential cross-border impact of incidents, a CTP should (where possible) also engage with financial sector incident response frameworks based outside of the UK, or which cover multiple jurisdictions.

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

5.52 A CTP should ensure that it shares relevant information with financial sector incident response frameworks during an incident, while taking appropriate steps to protect confidential or sensitive information (see Section 7).

Requirement 8: termination of services

5.53 A CTP must have in place appropriate measures to respond to a termination of any of its material services, including by putting in place:

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

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

- a change of control;
- a corporate reorganisation;
- insolvency;
- judicial, legal, political, and regulatory issues; or
- unrecoverable disruption.

5.55 For the purposes of Requirement 8, insolvency includes all insolvency proceedings that may affect a CTP's ability to continue delivering material services including but not limited to a company voluntary arrangement (CVA), administration, receivership, and liquidation. It also includes insolvency proceedings outside the UK.

5.56 Likewise, judicial, legal, political, and regulatory issues include legislative or regulatory changes, supervisory action (including enforcement), judicial rulings, sanctions etc.

5.57 As noted in section [3], firms and FMIs remain responsible for complying with existing requirements and expectations on operational resilience and outsourcing, and third party

risk management, including in relation to exit strategies.[21] Requirement 8 seeks to ensure that CTPs facilitate firms' and FMIs' compliance with these requirements, but does not replace them.

21 March 2021: **www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss**, Ch.10; and **www.bankofengland.co.uk/paper/2023/policy-on-outsourcing-and-third-party-risk-management-for-fmis**, Ch. 10 (February 2023).

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

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

- s312P FSMA;
- Chapter 5 of the Critical Third Parties Sourcebook in the FCA Handbook; and
- The following chapters in the Critical Third Parties Parts of the PRA and Bank Rulebooks:
  - Information-Gathering, evidence and testing;
  - self-assessment; and
  - information-sharing with firms.

General evidence and information requirement

6.2 A CTP must be able to demonstrate to the regulators its ability to comply with their rules. A CTP must provide some forms of evidence annually to the regulators, and other evidence upon request.

Self-assessment

6.3 A CTP must submit an annual, written self-assessment to the regulators demonstrating how they have complied with applicable requirements and expectations in the preceding year.

6.4 The self-assessment should set out the CTP's analysis of how they have met the requirements in the regulators' rules and the expectations set in this supervisory statement. The regulators expect the self-assessment to go through appropriate review and approval before a CTP submits it to them.

6.5 A CTP should ensure that its self-assessment is clear and concise. The CTP should make information referenced in the self-assessment (eg audit reports, certifications, test results

etc) available to the regulators upon request, but it is not necessary to include this information in the submission.

6.6 In line with CTP Fundamental Rule 6, a CTP's self-assessments should be balanced, thorough, and transparent. In particular, they should openly highlight identified vulnerabilities, areas for improvement, and proposed remediation. CTPs should use factual language and avoid an undue 'good news culture' when completing their self-assessments.

6.7 As noted in section 3, a CTP should submit its first self-assessment no later than three months following its initial designation by HM Treasury. The regulators accept that this initial self-assessment will be incomplete, and the CTP might be unable to demonstrate compliance with all the requirements in the regulators' rules. The purpose of this initial self-assessment is for the regulators to gauge the extent of a CTP's compliance with their rules at the point of designation and identify areas to prioritise in their first year of oversight. Following this initial submission, the CTP must submit a self-assessment annually.

6.8 A CTP must keep a copy of every annual self-assessment for a period of at least three years after submitting it to the regulators.

BOX 2: Information for CTPs to include in their self-assessment [22]

Risk management: demonstrate how the CTP's risk management framework and processes allow it to manage risks to its delivery of material services, including the ability to identify and escalate 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 from the entities and persons in its supply chain that are essential to its delivery of material services. The CTP should provide examples to demonstrate the due diligence it undertook, and the initial and ongoing assurance received from key Nth party service providers to help manage relevant risks.

Cyber and technology: demonstrate how the CTP is effectively identifying and managing risks to its 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 material service(s) it provides. The CTP should also show how its cyber resilience and security measures allow its technology to support, deliver, and maintain any material service. The CTP should also 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 material service(s) are planned, decided,

[22] As noted in the regulators' rules, the purpose of the self-assessment is for the CTP to demonstrate compliance with all the requirements in the regulators' rules. The information set out in Box 2 is designed to ensure that CTPs provide this information in a comparable, consistent and structured manner.

implemented, and operating effectively.

Mapping: demonstrate how the CTP has used mapping to:

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

Playbook: demonstrate how the CTP's financial sector incident management playbook can be used to mitigate risks to its customers and the wider impacts stemming from incidents that may adversely affect a CTP's material service. 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.

Termination: demonstrate that the CTP has appropriate measures in place to respond to a termination of its material service(s), including by putting in place

(i) transitional arrangements to support the effective, orderly, and timely termination of those services, and if applicable their transfer; and
(ii) provision for access, recovery and return of relevant assets (including data) to firms and FMIs.

The CTP should draw on examples (actual or hypothetical) to illustrate how it would support firms and FMIs in the event of a termination of its service(s);

Scenario testing: describe the CTP's strategy for testing its ability to deliver material services within their maximum tolerable level of disruption in severe but plausible scenarios. The CTP should explain how it selected and developed the scenarios used, the types of testing undertaken, and specify any scenarios under which the CTP could not continue to provide the material services within their maximum tolerable level of disruption.

Lessons learned: set out lessons learned from all types of testing, sector-wide exercises and 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.

Testing requirements

(a) Scenario testing

6.9 A CTP must carry out regular scenario testing of its ability to continue providing each of its material services within its maximum tolerable level of disruption in the event of a severe but plausible disruption to its operations.

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

6.11 A CTP's scenario testing should assume that disruption has occurred, and should not focus on preventing incidents from occurring, or considering the relative probability of

them occurring. This does not preclude CTPs from implementing controls to minimise the risk of incidents occurring and assessing the effectiveness of these controls through other means.

6.12 As noted in section 3, a CTP should carry out its first round of scenario tests no later than 12 months following its designation by HM Treasury, and regularly thereafter.

6.13 A CTP is responsible for identifying the scenarios it will test, taking into account:

- prior disruption to its services, operations, and supply chain; and
- risks and vulnerabilities identified in its mapping under Requirement 6 and other processes – a CTP should also use its map(s) and other relevant tools to calibrate the severity of the scenarios it tests (see section 4).

6.14 In line with Requirements 3-5, a CTP's scenario testing should regularly include one or more scenarios involving failure or disruption involving or relating to:

- its supply chain (eg infrastructure providers relied upon for the delivery of services);
- its technology and cyber resilience; or
- planned or hypothetical change management.

6.15 As with the operational resilience framework for firms and FMIs, there is no regulatory definition of a severe but plausible scenario for the purposes of this requirement on CTPs. However, the regulators recognise that it would not be proportionate to require CTPs to test their ability to continue providing material services within maximum tolerable levels of disruption in circumstances that are beyond severe or implausible.

6.16 If 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). For instance, by increasing the number or type of resources that become unavailable or the period for which they remain unavailable.

(b) Testing financial sector incident management playbooks

6.17 A CTP must test the measures in its financial sector incident management playbook annually with an appropriately representative sample of the firms and FMIs to which it provides material services.

6.18 A CTP should carry out its first test no later than 12 months following its initial designation by HM Treasury, and annually thereafter. If justified, the regulators could also

direct a CTP to re-test its playbook at a different time or more frequently than once a year. For instance, following significant disruption

6.19 Tests of a CTP's financial sector incident management playbook should be organised and coordinated by the CTP with participating firm and FMI customers.

A CTP must, as soon as reasonably practicable, prepare and send to the regulators a report of the test of its financial sector incident management playbook (including any actions taken in the light of the results of the test).

6.20 The report should set out:

- the key findings from the test;
- proposed revisions to the CTP's financial sector incident management playbook or the CTP's incident management more broadly as a result of the test; and
- general, non-attributable feedback to the CTP's firm and FMI customers based on the test eg on best practices identified.

6.21 A CTP should update the regulators on the implementation of any recommendations resulting from the latest test of its financial sector incident management playbook as soon as reasonably practicable.

Information provided by CTPs to the Regulators upon request

6.22 In addition to the self-assessment and testing requirements, CTPs must comply with ad-hoc requests for information by the regulators. The regulators will make these requests if appropriate, and on a risk-based approach. This section sets out how CTPs should comply with these requests (in line with CTP Fundamental Rule 6).

Audit reports, certifications etc

6.23 The regulators may ask a CTP for independent assurance reports or certifications of compliance with recognised standards.

6.24 However, audit reports, certifications etc have inherent limitations. In particular, they tend to focus on checklists of controls. Therefore, they can be of limited use for certain purposes, such as understanding how a CTP would deal with specific scenarios.

6.25 A CTP should therefore 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.

6.26 The regulators' information-gathering powers under s312P FSMA also enable the regulators to request information from a CTP and a Person Connected to a CTP.

Results of CTPs' internal tests

6.27 The Regulators may ask a CTP to share information relating to any internal tests it has carried out on its material services.

6.28 A CTP should 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

6.29 The regulators may ask a CTP to share information provided to other authorities, or the results of tests performed by or on behalf of these authorities. In this supervisory statement, 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. For instance, the Information Commissioner's Office (ICO).

6.30 A CTP should make this information available to the regulators as long as it is not legally prohibited. The regulators may also access this information directly from the relevant authorities subject to the existence of appropriate cooperation arrangements.

Collaborative testing

6.31 A CTP may be subject to or take part in collaborative testing by or on behalf of the firms and FMIs to which it provides material services eg scenario tests, pooled audits, and sector-wide exercises.

6.32 A CTP should make available to the regulators upon request the results of relevant collaborative tests or sector-wide exercises it undergoes or participates in.

Additional scenario tests

6.33 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. Additional scenario tests may be requested in response to a new risk or vulnerability. The regulators may identify these scenarios in collaboration with:

- firms and FMIs;
- financial sector incident response frameworks (see section [4]);

- non-UK financial authorities;
- standard-setting bodies and other international organisations;
- non-financial UK authorities; and
- industry experts.

Skilled person reviews

6.34 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:

- Chapter 12 of the Critical Third Parties sourcebook in the FCA Handbook;
- the 'Cost of Skilled Persons Reviews' and 'Contracts with Skilled Persons and delivery of reports' chapters in the Critical Third Parties Part of the PRA's and Bank's Rulebooks; and
- Joint Bank/PRA Supervisory Statement (see SSX/24 Reports by skilled persons: Critical Third Parties).

Sharing of assurance and testing information with firms and FMIs

6.35 A CTP must have effective and secure processes and procedures in place to ensure sufficient and timely information is given to firms and FMIs it provides services to in order to enable them to adequately manage risks related to their use of the CTP's services.

6.36 The information that a CTP must share with the firms and FMIs they provide services to includes the:

- results of testing performed in compliance with the regulators' requirements, including any action taken in the light of the results of the test; and
- a summary of the information contained in the CTP's annual self-assessment submitted to the regulators. The summary should be sufficiently clear and detailed to be useful to firms and FMIs, but need not include confidential or sensitive information in the full self-assessment submitted to the regulators.

6.37 A CTP is responsible for developing an appropriate method for sharing these summaries and other information with its firm and FMI customers. This method should include controls to ensure that confidential or sensitive information is appropriately protected.

7: Notifications

7.1 This section sets out how CTPs should comply with the incident notification requirements in:

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

7.2 The requirements referred to in para. [5.1] supplement the general requirement in CTP Fundamental Rule 6 for a CTP to be 'open and co-operative' with the regulators and disclose to them 'appropriately anything relating to the CTP of which they would reasonably expect notice' (see section 3).

7.3 A Where a CTP is required to disclose information under the regulators' rules that is subject to section 413 of FSMA (which deals with information subject to legal privilege), this information is not disclosable to the regulators. However, the CTP may choose whether or not to disclose this information to firms.

Relevant incident

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

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

7.5 The majority of relevant incidents are likely to result from an unplanned event or a series of unplanned linked events. For instance, a cyber-attack or a natural disaster. However, a planned event, such as a software update or change management programme (see Section 5), could also come under the definition of a relevant incident if it unexpectedly gave rise to the types of failure or disruption referred to in paragraph 7.4.

7.6 When assessing whether an incident meets the definition of a relevant incident, CTPs should take into account:

- Their internal assessment and classification of the incident;

- whether the incident warrants immediate and urgent action, including but not limited to escalation to its specialist teams, senior management, governing body etc (see paragraphs 5.32-5.37).

Phased approach to incident notifications

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

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

7.8 A CTP must also provide additional information about the incident to the regulators if requested.

7.9 A CTP should take reasonable steps to verify the information in their incident notifications ahead of submitting them. However, it should balance this against the need to notify the regulators, and the firms and FMIs it provides services to promptly enough for them to assess the potential impact and severity of the incident, and consider whether further action is warranted.

Format of incident notifications

7.10 A CTP would be able to use a range of formats for their notifications as long as these include the information specified in the regulators' rules and this supervisory statement. Alternatively, a CTP may share incident notifications or reports (or relevant parts thereof) submitted to:

- non-UK financial regulators;
- UK non-financial authorities eg:
  - the Information Commissioner's Office (ICO)[23] under the Network and Information Systems (NIS) Regulations 2018[24] or Data Protection Act 2018[25] (and future versions thereof); and
  - the National Cyber Security Centre (NCSC);[26] and
- its non-UK firm and FMI customers eg notifications to US banks under the Computer-Security Incident Notification rule.[27]

23 www.ico.org.uk.
24 www.legislation.gov.uk/uksi/2018/506.
25 www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
26 www.ncsc.gov.uk.
27 www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-55.html.

7.11 A CTP should also use its financial sector incident management playbooks and its engagement with financial sector incident response frameworks under Requirement 7 to ensure that incident notifications and other relevant information reach all firms and FMIs that use the affected material service(s) in a consistent, resource-efficient, and timely manner (see section 5).

Initial incident notifications

7.12 A CTP must submit an initial incident notification without undue delay after it becomes aware that it has experienced a relevant incident.

7.13 A CTP must send separate initial incident notifications to any firm and FMI customers that use the affected service(s) and the regulators.

7.14 Both notifications must include the following minimum information, so far as it is aware at the time of submission:

- the time when the incident was detected (in GMT or if different, the local time in the location where the relevant incident was detected);
- a description of the incident, which should include
  - the type eg cyber-attack, natural disaster etc; and
  - the nature and extent of the disruption eg complete or partial service failure, service(s) not performing as intended, data corruption, data loss etc.
- the cause or possible cause of the relevant incident, either known or suspected;
- contact details of any individual who is responsible for communicating with the firms to which the CTP provides services about the relevant incident (including the arrangements for coordinating responses to incidents affecting the financial sector referred to in Section 5);
- the name and number of material services affected;
- the nature and extent of the disruption and assets affected (actual and potential);
- details of any initial action taken or planned in response to the relevant incident;
- the geographical area affected by the relevant incident;
- the anticipated recovery time for each material service affected; and
- any other relevant information that will enable the firms and the Regulators to make an initial assessment of the relevant incident's potential impact.

7.15 In addition to the information referred to in Section 7, a CTP's initial incident notification to the regulators must also include the following information relating to the relevant

incident's potential impact on the stability of, or confidence in the UK's financial system (likewise in so far as they are aware at the time of the submission):

- the names and number of firms and FMIs affected;
- where assets relating or belonging to firms or FMIs have as a result of the relevant incident been lost, compromised, corrupted ,or become unavailable for a significant period, details of such matters;
- if applicable, contact details of any individual(s) responsible for communicating with the regulators about the relevant incident in addition to the regulators' central point of contact (see Section 5);
- details of any non-UK financial regulators and UK non-financial authorities that have also been notified of the relevant incident; and
- any other relevant information about the potential impact of the relevant incident on the stability of, or confidence in the UK's financial system.

Follow-up by the regulators

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

Intermediate incident notification

7.17 A CTP must keep the regulators, and the firms and FMIs that use the affected service(s) to, periodically informed with the following information in relation to the relevant incident (in so far as it is aware at the time of submission):

- suitable technical information that assists in understanding the nature of the relevant incident;
- steps taken to restore the services or recover the assets;
- information about the Critical Third Party's stakeholder engagement;
- information about any ongoing investigation;
- in relation to cyber-attacks:
  - the type of threat actor (including known capabilities and motives); and
  - the complexity and novelty of the attack;
  - the potential impact of mainstream and social media coverage on the CTP and firms (including as a result of misinformation and disinformation); and
- any update on information previously provided to the recipient of the notice or any other information which appears to the CTP reasonably relevant to the recipient of the notice.

7.18 CTPs' intermediate incident notifications to the regulators must also include the following information in relation to the relevant incident:

- any vulnerabilities that the relevant incident has exposed the CYP, other CTPs or firms to, or which have otherwise been revealed;
- whether there is a risk of similar incidents happening at other CTPs or third party service providers to firms and FMIs, due to issues caused by the relevant incident or by factors in common with the relevant incident.

7.19 The updates on any information previously provided should be sent:

- both to the regulators and the firms and FMIs the CTP provides the affected service(s) to if the update relates to information mentioned in para 7.14;
- only to the regulators if the update relates to information in para 7.15.

7.20 The frequency, level of detail and timing of submission of these intermediate notifications should balance the competing needs of the:

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

7.21 If requested to do so by the regulators, a CTP must provide intermediate notifications at a time or frequency specified by the regulators. The regulators may choose to use their information gathering powers or powers of direction.

7.22 If a CTP resolves an incident before an intermediate notification(s) is due, or before the regulators request it, it can move straight to the financial incident notification phase.

7.23 A CTP can the same use updates to other customers or authorities as long as they include the information required in the regulators' rules.

Final incident notification

7.24 Once a relevant incident has been resolved and the CTP has had time to assess its root causes and identify lessons learned, it must provide the regulators, and the firms and FMIs to which it provides the affected service(s), with a final incident notification with the following information:

- a description of the root cause(s) of the relevant incident;
- a description of any remedial actions the CTP has put, or is planning to put, in place as a result of the incident, including an estimated timeline for completion of these actions;
- a description of identified areas for improvement for:

    - the CTP; and
    - the firms and FMIs it provides services (on an anonymised, general basis).
  - the CTP's assessment of the likelihood of the relevant incident reoccurring, and its long-term implications on its services and, to the extent known, similar service provided by other third parties; and
  - any other information which appears relevant.

7.25 A CTP must take reasonable steps to identify and obtain the necessary information to enable it to comply with the obligations in this Chapter

Other notification requirements

7.26 In addition to the incident notification requirements examined in the previous sections, a CTP must also notify the regulators promptly where:

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

7.27 CTPs must submit all notifications by electronic means where possible. If electronic means are not available, CTPs should use other appropriate, available means.

Inaccurate, false, or misleading information

7.28 A CTP must take all reasonable steps to ensure that all information it gives to the regulators in accordance with the requirements referred to in this section, is:

- factually accurate or, in the case of estimates and judgements, fairly and properly based after making appropriate enquiries; and
- complete, in that it should include anything of which the regulator would reasonably expect notice.

7.29 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.

7.30 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 relevant incident, this can be done in the intermediate updates discussed above;
- an explanation why such information was or may have been provided; and
- the correct information.

7.31 If the information in para 7.24 cannot be submitted with the notification (because it is not immediately available), it must instead be submitted as soon as possible afterwards.

8: Public references to a CTP's designated status

Public references to a CTPs' designated status

8.1 HMT designates CTPs by regulations (s312L(1) FSMA), which will be publicly available. HMT will also maintain a list of all designated CTPs.

8.2 A CTP must avoid any indications (by itself or anyone acting on its behalf) that it has the regulators' endorsement or that designation means its services are superior.

8.3 Likewise, a CTP (by itself or anyone acting on its behalf) must not in any communication suggest designation or oversight confers any advantage to a firm or anyone else in using its services as compared to a service provider who is not designated.

8.4 The relevant rules are located in:

- Chapter 13 of the Critical Third Parties Sourcebook in the FCA Handbook; and
- The 'Referrals for approval by the regulators or designation by HMT' and chapters of the Critical Third Parties Parts of the PRA and Bank Rulebooks.

9: Nomination of legal person

9.1 A CTP which is headquartered outside the UK must nominate a legal person in the UK to perform certain functions, such as receiving statutory notices under FSMA and other documents from the regulators.

9.2 This requirement applies in addition to the requirement to nominate a staff member to act as the central point of contact for the Regulators under Requirement 1 (see section 5).

9.3 The term 'person' is as defined in Schedule 1 of the Interpretation Act 1978 and 'includes a body of persons corporate or unincorporate'. For the purposes of this requirement:

- a CTP that is headquartered outside the UK, but has a UK subsidiary should use its as its nominated legal person in the UK;
- a CTP that is headquartered outside the UK and has no UK subsidiary should appoint suitable UK-based corporate body, partnership or limited liability partnership (eg a law firm) as its representative.

9.4 The relevant rules are located in:

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

10. Record keeping and emergency relief

10.1 The regulators propose that a CTP must arrange for orderly records to be kept of its business and internal organisation, in so far as it concerns the provision of services to firms or FMIs. These records must be sufficient to enable each regulator to:

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

10.2 The relevant rules are located in:

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