PRA RULEBOOK: CRITICAL THIRD PARTIES INSTRUMENT 2024

Powers exercised

A. The Prudential Regulation Authority ("PRA") makes this instrument in the exercise of the following powers and related provisions in the Financial Services and Markets Act 2000 ("the Act"):

(1) section 137T (General supplementary powers);
(2) section 166(9) (Reports by skilled persons);
(3) section 166A(9) (Appointment of skilled person to collect and update information);
(4) section 312M (Power to make rules);
(5) section 312P (Information gathering and investigations); and
(6) paragraph 31 (Fees) of Part 3 (Penalties and Fees) of Schedule 1ZB (The Prudential Regulation Authority).

B. The rule-making powers referred to above are specified for the purpose of section 138G(2) (Rule-making instruments) of the Act.

PRA Rulebook: Critical Third Parties Instrument 2024

C. The PRA makes the rules in the Annexes to this instrument.

Part	Annex
Glossary	A
Critical Third Parties	B
Fees	C
Interpretation	D

Commencement

D. This instrument comes into force on 1 January 2025.

Citation

E. This instrument may be cited as the PRA Rulebook: Critical Third Parties Instrument 2024.

By order of the Prudential Regulation Committee
8 November 2024

Annex A

Amendments to the Glossary Part

In this Annex new text is underlined and deleted text is struck through.

…

critical third party

means a *person* designated by the *Treasury* in regulations made under section 312L(1) of *FSMA*.

…

firm

(except in the Critical Third Parties Part of the *PRA* Rulebook) means a *PRA-authorised person* within the meaning of section 2B(5) of *FSMA*.

(in the Critical Third Parties Part of the *PRA* Rulebook) means:

(1) an *authorised person*;

(2) a *relevant service provider*; or

(3) an *FMI entity*.

…

person connected with a critical third party

has the same meaning as in section 312P(10) of *FSMA*, and the reference to any relevant time means any time relevant for the application of the relevant rule.

…

skilled person

(except in the Critical Third Parties Part of the *PRA* Rulebook) means a *person* appointed to:

(1) make and deliver to the *PRA* a report as provided for by section 166 of *FSMA* (Reports by skilled persons); or

(2) collect or update information as required by the *PRA* under section 166A of *FSMA* (Appointment of skilled person to collect and update information).

(in the Critical Third Parties Part of the *PRA* Rulebook) means a *person* appointed to:

(1) make and deliver to a *regulator* a report as provided for by section 166 of *FSMA* (Reports by skilled persons) (as applied by section 312P of *FSMA*); or

(2) collect or update information as required by a *regulator* under section 166A of *FSMA* (Appointment of skilled person to collect and update information) (as applied by section 312P of *FSMA*).

…

Annex B

Critical Third Parties Part

In this Annex, the text is all new and is not underlined.

Part

CRITICAL THIRD PARTIES

Chapter content

1 APPLICATION AND DEFINITIONS

1.1 Unless otherwise stated, this Part applies to a *critical third party* in connection with the provision of *services* wherever those *services* are carried out.

1.2 In this Part, the following definitions shall apply:

affected firm

means, in relation to a *CTP operational incident*:

(1) any *firm* to which the *critical third party* supplies a *systemic third party service* impacted by that *CTP operational incident*; or

(2) any *firm* whose *assets* are, or may be, seriously and adversely impacted by that *CTP operational incident*.

asset

means something, whether tangible or intangible, that is of value, including people, data, information, infrastructure, finances and reputation.

Bank

means the *Bank of England*, other than when it is acting in its capacity as the *PRA*.

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.

CTP duties

means the duties and obligations placed upon a *critical third party* by or under *FSMA*, including the rules in this Part.

CTP Fundamental Rules

means the rules set out in 3.1 to 3.6.

CTP operational incident

means either a single event or a series of linked events that:

(1) causes serious *disruption* to the delivery of a *systemic third party service*; or

(2) impacts the *critical third party's* operations such that the availability, authenticity, integrity or confidentiality of *assets* belonging to *firms* which a *critical third party* 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.

disruption

includes, in relation to a *systemic third party service*:

(1) complete or partial failure of that *service*;

(2) complete or partial degradation to the quality of that *service*;

(3) complete or partial unavailability of that *service*; or

(4) the *service* not performing as intended as a whole or in part.

incident management playbook

means a *document* setting out at least the matters required by 4.10(3).

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 *critical third party's incident management playbook*.

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*.

oversight function

means a function conferred by *FSMA* on a *regulator* in relation to *critical third parties*.

regulator

means:

(1) the *PRA*;

(2) the *FCA*; or

(3) the *Bank*,

and 'regulators' means the *PRA*, the *FCA* and the *Bank*.

relevant document

has the meaning given in regulation 1 of the Financial Services and Markets Act 2000 (Service of Notices) Regulations 2001 (SI 2001/1420).

supply chain

means the network of *persons* that provide infrastructure, goods, *services* or other inputs directly or indirectly used by a *critical third party* to deliver, support or maintain a *systemic third party service*.

systemic third party service

means a *service* (wherever carried out) provided by a *critical third party* 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.

2 INTERPRETATIVE PROVISIONS

2.1 Unless the contrary intention appears, any reference in this Part to a *regulator* or the *regulators* is a reference:

(1) when the relevant *oversight function* is exercised by the *PRA*, to the *PRA*;

(2) when the relevant *oversight function* is exercised by the *FCA*, to the *FCA*;

(3) when the relevant *oversight function* is exercised by the *Bank*, to the *Bank*.

3 CRITICAL THIRD PARTY FUNDAMENTAL RULES

3.1 *CTP Fundamental Rule* 1: A *critical third party* must conduct its business with integrity.

3.2 *CTP Fundamental Rule* 2: A *critical third party* must conduct its business with due skill, care and diligence.

3.3 *CTP Fundamental Rule* 3: A *critical third party* must act in a prudent manner.

3.4 *CTP Fundamental Rule* 4: A *critical third party* must have effective risk strategies and risk management systems.

3.5 *CTP Fundamental Rule* 5: A *critical third party* must organise and control its affairs responsibly and effectively.

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

3.7

(1) 3.6 applies to a *critical third party* in respect of a *critical third party's* provision of any *services* to *firms*; and

(2) 3.1 to 3.5 only apply to *a critical third party* in respect of the *critical third party's* provision of *systemic third party services* to *firms*.

4 OPERATIONAL RISK AND RESILIENCE REQUIREMENTS

4.1 A *critical third party* must have in place sound, effective and comprehensive strategies, controls, processes and systems that enable it to comply with this Part.

4.2 The strategies, processes and systems required by 4.1 must be proportionate to the nature, scale and complexity of the *critical third party's* activities.

Requirement 1: Governance

4.3 A *critical third party* 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 *critical third party* 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 of 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 *critical third party's* ability to prevent, respond and adapt to, as well as recover from, any *CTP operational incident*;

(4) implementing lessons learned 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.

Requirement 2: Risk management

4.4 A *critical third party* 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 5.

Requirement 3: Dependency and supply chain risk management

4.5 A *critical third party* must (as part of its obligation under 4.4) identify and manage any risks to its *supply chain* that could affect its ability to deliver a *systemic third party service*.

4.6 A *critical third party* must take reasonable steps to ensure that its *key nth-party providers* and *persons connected with a critical third party* that are part of its *supply chain*:

(1) are informed of the *CTP duties* that apply to the *critical third party*;

(2) cooperate with the *critical third party* in meeting those *CTP duties*; and

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

Requirement 4: Technology and cyber resilience

4.7 A *critical third party* must (as part of its obligation under 4.4) 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 4.1) 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 5) and processes and measures that reflect lessons learned from that testing and exercising.

Requirement 5: Change management

4.8 A *critical third party* 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.

Requirement 6: Mapping

4.9 A *critical third party* must:

(1) within 12 *months* of being designated by the *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).

Requirement 7: Incident management

4.10 A *critical third party* must manage effectively *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 *critical third party* being designated by the *Treasury*, which sets out the plans and procedures to be followed by the *critical third party* 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*.

Requirement 8: Termination of a systemic third party service

4.11 A *critical third party* must have in place appropriate measures to respond to a termination of any of its *systemic third party service*s (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.

5 ASSURANCE, SCENARIO TESTING AND INCIDENT MANAGEMENT PLAYBOOK EXERCISE

General evidence requirement

5.1 A *critical third party* must be able to demonstrate to the *regulators* its ability to comply with this Part.

Scenario testing

5.2 As part of its obligation under 5.1, a *critical third party* 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* (set in accordance with 4.10(2)) in the event of a severe but plausible disruption to its operations.

5.3 When carrying out the scenario testing required by 5.2, a *critical third party* 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 *systemic third party service* in those circumstances.

Incident management playbook exercise

5.4 As part of its obligation under 5.1, a *critical third party* must assess the effectiveness of its *incident management playbook* regularly, including undertaking an appropriate *incident management playbook exercise* with a representative sample of the *firms* to which it provides *systemic third party services* within 12 *months* of the *critical third party* being designated by the *Treasury* and at least biennially thereafter.

5.5 A *critical third party* must, as soon as is practicable, prepare and submit to the *regulators* a report of the *incident management playbook exercise* undertaken under 5.4 (including any actions taken in the light of the results of that exercise).

6 SELF-ASSESSMENT

6.1 A *critical third party* must provide to the *regulators*:

(1) within three *months* of the *critical third party* being designated by the *Treasury*, an interim self-assessment; and

(2) annually thereafter, an annual self-assessment,

of the *critical third party's* compliance with this Part.

6.2 A *critical third party* must keep a copy of each interim and annual self-assessment referred to in 6.1 for a period of at least three years after submitting it to the *regulators*.

7 INFORMATION SHARING WITH FIRMS

7.1 A *critical third party* must 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 *critical third party's systemic third party services*.

7.2 The information referred to in 7.1 includes, but is not limited to:

(1) results of testing and exercising carried out in accordance with 5 (including any action taken in the light of the results of the testing and exercising);

(2) the annual self-assessment prepared in compliance with 6.1(2), redacted as appropriate; and

(3) the appropriate maximum tolerable level of *disruption* set by the *critical third party* in accordance with 4.10(2) for each *systemic third party service* provided to the *firm*.

8 INCIDENT REPORTING

Initial incident report

8.1 A *critical third party* 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 the following information about the *CTP operational incident*:

(1) to the *regulators* and to *affected firms*:

(a) a description of the *CTP operational incident*, including:

(i) the nature and extent of:

(1) the *disruption* to *systemic third party services*; or

(2) impact to the *critical third party's* operations;

(ii) the time when the *CTP operational incident* was detected (and, if different, the local time in the location where the *CTP operational incident* was detected);

(iii) the name and number of *systemic third party services* affected;

(iv) the geographical area, including the jurisdictions, affected by the *CTP operational incident*; and

(v) if known, the cause of the *CTP operational incident*;

(b) contact details of any individual who is responsible for communicating with the *affected firms* about the *CTP operational incident*;

(c) details of any initial action taken or planned in response to the *CTP operational incident*;

(d) 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

(e) any other information the *critical third party* 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*,

and

(2) to the *regulators*:

(a) the names of the *affected firms*;

(b) the names of any other regulatory body or authorities (other than the *regulators*) that have been notified of the *CTP operational incident*; and

(c) any other information that the *critical third party* reasonably considers will assist the *regulators* in making an initial assessment of the impact the *CTP operational incident* could have on the stability of, or confidence in, the *UK's* financial system.

Intermediate incident report

8.2 A *critical third party* must, as soon as is practicable after any significant change in circumstances from that described in the initial report submitted under 8.1 and any intermediate incident report already submitted under this rule (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 information further to that already disclosed in relation to the *CTP operational incident*, including but not limited to:

(1) any information that the *critical third party* reasonably considers will assist the *regulators* and *affected firms* in understanding the nature and extent of the *CTP operational incident*;

(2) any steps taken to resolve the *CTP operational incident*;

(3) if the *CTP operational incident* has been resolved, the time and date it was resolved; and

(4)

(a) any other information the *critical third party* reasonably considers to be relevant to *affected firms*; and

(b) to the *regulators* only, any other information the *critical third party* reasonably considers to be relevant to the *regulators*.

Final incident report

8.3 A *critical third party* must, within a reasonable time of the *CTP operational incident* being resolved, provide the *regulators* and the *affected firms* with the following information in relation to the *CTP operational incident*:

(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 *critical third party* has or is planning to put in place and an estimated timeline for the completion of those remedial actions;

(4) a description of the *critical third party's* assessment of:

(a) the likelihood of recurrence of the *CTP operational incident*; and

(b) the long-term implications of the *CTP operational incident*;

(5) a description of identified areas for improvement for the *critical third party* and, where relevant, the *affected firms*; and

(6)

(a) any other information the *critical third party* reasonably considers to be relevant to *affected firms*; and

(b) to the *regulators* only, any other information the *critical third party* reasonably considers to be relevant to the *regulators*.

9 NOTIFICATIONS

9.1 A *critical third party* 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 *critical third party's* ability to deliver any of its *systemic third party services* or meet any of its obligations under this Part, including where:

(1) civil proceedings are brought by or against the *critical third party* or a claim or dispute is referred to alternative dispute resolution in any jurisdiction;

(2) disciplinary measures or sanctions have been imposed on the *critical third party* by any statutory or regulatory authority in any jurisdiction (other than the *regulators*), or the *critical third party* becomes aware that one of those authorities has commenced an investigation into its affairs;

(3) the *critical third party* 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

(4) the *critical third party* is subject to criminal proceedings, or has been prosecuted for, or convicted of, a criminal offence in any jurisdiction involving fraud or dishonesty.

10 INACCURATE, FALSE OR MISLEADING INFORMATION

10.1 A *critical third party* 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 by 8 and 9) is:

(1) factually accurate or, in the case of estimates and judgements, fairly and properly based after appropriate enquiries have been made by the *critical third party*; and

(2) complete, in that it should include anything of which the *regulators* would reasonably expect notice.

10.2 If a *critical third party* is unable to obtain the information required in 10.1, then it must inform the *regulators* that the scope of the information provided is, or may be, limited.

10.3 If a *critical third party* 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.

10.4 Subject to 10.5, the notification required by 10.3 must include:

(1) details of the information which is or may be false, misleading, incomplete or inaccurate, or has or may have changed;

(2) an explanation of why such information was or may have been provided; and

(3) the correct information.

10.5 If the information in 10.4(3) cannot be submitted with the notification (because it is not immediately available), it must instead be submitted as soon as is practicable afterwards.

11 ADDRESS FOR SERVICE

11.1 A *critical third party* must provide the *regulators* with an address in the *UK* for the service of *documents* (including *relevant documents*).

11.2 A *critical third party* must notify the *regulators* of any change to the information provided under 11.1 as soon as is practicable.

12 CONTRACTS WITH SKILLED PERSONS AND DELIVERY OF REPORTS

12.1 If a *critical third party* appoints a *skilled person*, that *critical third party* must give the *regulators* sufficient and timely information about the cost of the *skilled person's* report or collection or updating of information, including both an initial estimate of the cost as well as the cost of the completed report, collection or updating of information.

12.2 When a *critical third party* appoints a *skilled person*, the *critical third party* must, in a contract with that *person*:

(1) require and permit the *skilled person* during and after the course of their appointment:

(a) to cooperate with the *regulators* in connection with the discharge of their *oversight functions*; and

(b) to communicate to the *regulators* information on, or the *skilled person's* opinion on, matters of which they have, or had, become aware in their capacity as a *skilled person* reporting on the *critical third party* in the following circumstances:

(i) the *skilled person* reasonably believes that the information on, or their opinion on, matters for which they were appointed may be of material significance to the *regulators* in determining whether the *critical third party* concerned complies with and will continue to comply with the *CTP duties*; or

(ii) the *skilled person* reasonably believes that the *critical third party* is not, may not be or may cease to be a going concern;

(2) require the *skilled person* to prepare a report or collect or update information, as notified to the *critical third party* by the *regulator* that has required such report, collection or updating within the time specified by the *regulator*; and

(3) waive any contractual or other duty of confidentiality owed by the *skilled person* to the *critical third party* which might limit the provision of information or opinion by that *skilled person* to the *regulators* in accordance with (1) or (2).

12.3 A *critical third party* must ensure that the contract it makes with the *skilled person* under 12.2 requires and permits the *skilled person* to provide the following to the *regulators* if requested to do so:

(1) interim reports;

(2) source data, *documents* and working papers;

(3) copies of any draft reports given to the *critical third party*; and

(4) specific information about the planning and progress of the work to be undertaken (which may include project plans, progress reports including percentage of work completed, details of time spent, costs to date, and details of any significant findings and conclusions).

12.4 A *critical third party* must ensure that the contract required by 12.2 is:

(1) governed by the laws of a part of the *UK*;

(2) in writing, and:

(a) expressly provides that the *regulators* have a right to enforce the provisions included in the contract under 12.2, 12.3 and 12.4(2)(b) to (d);

(b) expressly provides that, in proceedings brought by the *regulators* for the enforcement of those provisions, the *skilled person* is not to have available by way of defence, set-off or counterclaim any matter that is not relevant to those provisions;

(c) if the contract includes an arbitration agreement, expressly provides that the *regulators* are not, in exercising the right in (a), to be treated as a party to, or bound by, the arbitration agreement; and

(d) expressly provides that the provisions included in the contract under 12.2, 12.3 and 12.4(2) are irrevocable and may not be varied or rescinded without the *regulators'* consent; and

(3) not varied or rescinded in such a way as to extinguish or alter the provisions referred to in (2)(d).

12.5 When a *critical third party* appoints a *skilled person*, a *critical third party* must take reasonable steps to ensure that the *skilled person* delivers a report or collects or updates information in accordance with the terms of the *skilled person's* appointment.

12.6 A *critical third party* must provide all reasonable assistance to a *skilled person* appointed to provide a report under section 166 of *FSMA* (Reports by skilled persons) or to collect or update information under section 166A (Appointment of skilled person to collect and update information) of *FSMA* (as applied by section 312P of *FSMA*) and take reasonable steps to ensure that its *employees* and agents also provide all reasonable assistance to that *skilled person*.

13 REFERRING TO OVERSIGHT BY THE REGULATORS OR TREASURY DESIGNATION

13.1 A *critical third party* 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 *critical third party* has the approval or endorsement of any of the *regulators* by virtue of:

(1) its designation as a *critical third party*; or

(2) being overseen by the *regulators* in respect of *services* it provides to *firms*.

13.2 A *critical third party* must not, and must take reasonable steps to ensure that any *person* acting on its behalf does not, in any communication indicate or imply that the *critical third party's* designation by the *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 *critical third party*.

13.3 13.1 and 13.2 do not prevent the making of statements that explain, in a way that is fair, clear and not misleading:

(1) that the *critical third party* has been designated by the *Treasury*;

(2) that the *critical third party* is subject to oversight by the *regulators* in respect of the *systemic third party services* it provides to *firms*; and

(3) the *systemic third party services* the *critical third party* provides to *firms*.

14 RECORD KEEPING

14.1 A *critical third party* must arrange for orderly records to be kept of its business and internal organisation, in so far as they concern the provision of *systemic third party services* to *firms*, which must be sufficient to enable each *regulator* to:

(1) perform its *oversight functions*; and

(2) ascertain whether or not the *critical third party* has complied with its *CTP duties*.

15 ELECTRONIC SUBMISSION OF INFORMATION

15.1 A *critical third party* must submit the information required under this Part to the *regulators* and *affected firms* (as the context requires) by electronic means.

Annex C

Amendments to the Fees Part

In this Annex new text is underlined and deleted text is struck through.

…

4 REGULATORY TRANSACTION FEES

…

4.16 Where the *PRA* has given notice to a *fee payer* of its intention to itself appoint a *skilled person* to:

(1) provide it with a report pursuant to section 166(3)(b) of *FSMA* (including as applied by section 312P of *FSMA*); or

(2) collect or update information pursuant to ~~S~~section 166A(2)(b) of *FSMA* (including as applied by section 312P of *FSMA*);

the fee will be the amount invoiced by the ~~skilled person~~*skilled person*.

[Note: section 312P of *FSMA* applies section 166 of *FSMA* (Reports by skilled persons) in relation to *critical third parties* and *persons connected with critical third parties* and applies section 166A of *FSMA* in relation to *critical third parties*]

4.17 The *due date for payment* by the *firm*, *critical third party* or *person connected with a critical third party* is 30 days from the date of each invoice from the *PRA* to the *firm*, *critical third party* or *person connected with a critical third party*.

…

Annex D

Amendments to the Interpretation Part

In this Annex new text is underlined and deleted text is struck through.

1 APPLICATION

1.1 Unless otherwise stated, this Part applies to:

…

(4) a *PRA approved parent holding company*; ~~and~~

(5) a *PRA designated parent holding company* ~~.~~;

(6) a *critical third party*; and

(7) a *person connected with a critical third party*.

…

Glossary externally defined terms

Term	Definition source
authorised person	section 417(1) of *FSMA*
document	section 417(1) of *FSMA*
FMI entity	section 312L(8) of *FSMA*
month	Schedule 1, Interpretation Act 1978
relevant service provider	section 312L(8) of *FSMA*
service	section 312L(8) of *FSMA*
Treasury	Schedule 1, Interpretation Act 1978