PRA RULEBOOK: NON-AUTHORISED PERSONS: 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); and
(4) section 312M (Power to make rules).

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

PRA Rulebook: Non-Authorised Persons: Critical Third Parties Instrument 2024

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

Commencement

D. This instrument comes into force on [DATE].

Citation

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

By order of the Prudential Regulation Committee
[DATE]

Annex

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 every *Critical Third Party.*

1.2 In this Part, the following definitions shall apply:

asset

includes data, people, information, and infrastructure.

authorised person

has the same meaning as in section 31 of *the Act*.

Bank

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

Critical Third Party

means a person that is designated by the *Treasury* by regulations made in exercise of the power in section 312L(1) of *the Act*.

CTP duties

means the duties and obligations placed upon a *Critical Third Party* by or as a result of *the Act*, including the rules in this Part.

CTP Fundamental Rules

means the rules set out in 3.1 to 3.6.

document

means information recorded in any form and, in relation to information recorded otherwise than in legible form, references to its production include references to producing a copy of the information in legible form or in a form from which it can readily be produced in visible and legible form.

disruption

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

employee

means an individual:

(1) who is employed or appointed by a *Critical Third Party* in connection with its business, whether under a contract of service or for services or otherwise; or

(2) whose services, under an arrangement between that *Critical Third Party* and a third party, are placed at the disposal and under the control of the *Critical Third Party*.

FCA

means the Financial Conduct Authority.

Fee payer

means any *Critical Third Party* or *person connected with a Critical Third Party* required to pay a fee in accordance with Chapter 11.

Financial Sector Incident Management Playbook

means a document setting out how a *Critical Third Party* will communicate with and support the *Regulators* and *firms* (individually and collectively) in respect of incidents that affect the delivery of a *material service*.

Firm

means:

(1) an *authorised person*;

(2) a *relevant service provider*; or

(3) an *FMI entity*.

FMI entity

has the same meaning as in section 312L(8) of *the Act*.

governing body

means the board of directors, committee of management or other governing body of a *Critical Third Party.*

Key Nth-party service provider

means a person that is part of a *Critical Third Party's supply chain* and is essential to the ultimate delivery of a *material service* to one or more *firms.*

material 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.

oversight functions

means any of the functions conferred by *the Act* upon a *Regulator* in relation to *Critical Third Parties*.

person connected with a Critical Third Party

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

PRA

means the Prudential Regulation Authority.

Regulator

means:

(1) the *PRA*;

(2) the *FCA*; or

(3) the *Bank*.

and *Regulators* means them collectively.

relevant service provider

has the same meaning as in section 312L(8) of *the Act*.

skilled person

means a person appointed to:

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

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

supply chain

means the network of persons that provide infrastructure, goods, services or other inputs directly or indirectly utilised by a *Critical Third Party* to deliver, support or maintain a *material service*.

the Act

means the Financial Services and Markets Act 2000.

Treasury

has the same meaning as in Schedule 1 of the Interpretation Act 1978.

UK

means the United Kingdom.

2 INTERPRETATIVE PROVISIONS

2.1 Unless the contrary intention appears any reference in this Part to a *Regulator* is a reference to:

(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 a *Regulator* in an open and cooperative way, and must disclose to a *Regulator* appropriately anything relating to the *Critical Third Party* of which it would reasonably expect notice.

3.7 The *CTP Fundamental Rules* apply with respect to a *Critical Third Party* carrying on the activity of providing services to *firms* wherever those services are carried out.

4 CRITICAL THIRD PARTIES 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 the other rules in this Part.

Requirement 1: Governance

4.2 A *Critical Third Party* must ensure that its governance arrangements promote the resilience of any *material service* it provides, including by:

(1) appointing a natural person that is an employee or member of its governing body (who 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*;

(2) establishing clear roles and responsibilities at all levels of its staff involved in the delivery of a *material 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 event that causes *disruption* to the delivery of a *material service*, and learn from those events and any testing undertaken;

(4) ensuring appropriate review and approval of any information provided to the *Regulators*;

(5) notifying the *Regulators* in writing of:

(a) the name of the person appointed under (1);

(b) the business address of that person; and

(c) email addresses, telephone numbers and out of hours contact details for that person; and

(6) notifying the *Regulators* of any changes to the information notified under 4.2(5) as soon as practicable.

Requirement 2: Risk management

4.3 A *Critical Third Party* must effectively manage risks to its ability to continue to deliver a *material service* including by:

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

(2) ensuring that it has 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) a *disruption* to a *material service*;

(b) engagement with the *Regulators*;

(c) new and emerging risks; and

(d) any associated testing, including but not limited to testing carried out in accordance with Chapter 5.

Requirement 3: Dependency and supply chain risk management

4.4 A *Critical Third Party* must (as part of its obligation under 4.3) identify and manage any risks to its *supply chain* that could affect its ability to deliver a *material service*, including due to dependencies on:

(1) a *person connected with a Critical Third Party*; or

(2) a *Key Nth-party service provider*.

4.5 A *Critical Third Party* must take all reasonable steps to ensure that each person in its *supply chain*:

(1) understands the requirements that apply to the *Critical Third Party* by virtue of the *CTP duties*;

(2) takes appropriate action to facilitate the *Critical Third Party* meeting those requirements; and

(3) provides the *Regulators* with access to any information relevant to them exercising their *oversight functions*.

Requirement 4: Technology and Cyber resilience

4.6 A *Critical Third Party* must (as part of its obligation under 4.3) ensure the resilience of any technology that delivers, maintains or supports a *material service*, including by having:

(1) technology and cyber risk management and operational resilience measures;

(2) regular testing of those measures (including as part of its obligations under Chapter 5);

(3) processes and measures that reflect lessons learned from testing (including under (2)); and

(4) processes and procedures that convey relevant and timely information to assist risk management and decision-making processes.

Requirement 5: Change management

4.7 A *Critical Third Party* 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:

(1) implementing appropriate policies, procedures and controls to ensure the resilience of any change to a *material service*;

(2) implementing any change to a *material service* in a way that minimises the risk of undue *disruption*; and

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

Requirement 6: Mapping

4.8 A *Critical Third Party* must:

(1) (subject to (2)) identify and document:

(a) resources, including the *assets*, and technology, used to deliver, support, and maintain each *material 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) have completed the identification and documentation of resources under (1) within 12 months of the *Critical Third Party* being designated by the *Treasury* and keep it up to date at all times thereafter.

Requirement 7: Incident management

4.9 A *Critical Third Party* must appropriately manage incidents that adversely affect, or may reasonably be expected to adversely affect, the delivery of a *material service* including by:

(1) implementing appropriate measures to respond to and recover from incidents in a way that minimises the impact;

(2) setting a maximum tolerable level of disruption to the service;

(3) maintaining and operating a *Financial Sector 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*; and

(4) coordinating and engaging 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.

Requirement 8: Termination of a material service

4.10 A *Critical Third Party* must have in place appropriate measures to respond to a termination of any of its *material 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, recovery and return of any relevant *assets* to the *firms* it provides that service to and where applicable in an easily accessible format.

5 INFORMATION GATHERING, EVIDENCE AND TESTING

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 *material service* within its maximum tolerable level of disruption in the event of a severe but plausible disruption.

5.3 When carrying out the scenario testing, 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 *material service* in those circumstances.

Testing of Financial Sector Incident Management Playbooks

5.4 As part of its obligation under 5.1, a *Critical Third Party* must test the measures in its *Financial Sector Incident Management Playbook* annually with an appropriate representative sample of the *firms* to which it provides *material services*.

5.5 A *Critical Third Party* must, as soon as reasonably practicable, prepare and send to the *Regulators* a report of the test undertaken under 5.4 (including any actions taken in the light of the results of the test).

6 SELF-ASSESSMENT

6.1 A *Critical Third Party* must prepare an annual written self-assessment for the *Regulators* of its compliance with this Part.

6.2 The self-assessment must be submitted to the *Regulators* within three months of a *Critical Third Party* being designated by the *Treasury* and thereafter within 12 months of the last submission.

6.3 A *Critical Third Party* must keep a copy of its annual self-assessment 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 effective and secure processes and procedures in place to ensure sufficient and timely information is given to a *firm* to which it provides any services to enable that *firm* to adequately manage risks related to its use of the *Critical Third Party's* services.

7.2 The information referred to in 7.1 includes:

(1) results of testing carried out (including any action taken in the light of the results of the test) in compliance with Chapter 5; and

(2) a summary of the information contained in the annual self-assessment made in compliance with Chapter 6.

8 NOTIFICATIONS

8.1 In this Chapter, a relevant incident is either a single event or a series of linked events that:

(1) causes serious *disruption* to the delivery of a *material service*;

(2) seriously and adversely impacts the availability, authenticity, integrity or confidentiality of *assets* relating or belonging to *firms* which a *Critical Third Party* has access to as a result of it providing services to those *firms* or results in a serious loss of such *assets*; or

(3) has the potential to result in any of those things.

Initial Incident Notifications

8.2 Subject to 8.8, a *Critical Third Party* must, in so far as it is aware at the time of submission of a notification under this rule, provide the *Regulators* and the *firms* it provides the affected service to with the following information about the relevant incident:

(1) the time when the incident was detected (in GMT or if different, the local time in the location where the relevant incident was detected);

(2) a description of the relevant incident;

(3) the cause or possible cause of the relevant incident, either known or suspected;

(4) contact details of any individual who is responsible for communicating with the *firms* to which the *Critical Third Party* provides services about the relevant incident;

(5) the name and number of *material services* affected;

(6) the nature and extent of the *disruption* and *assets* affected (actual and potential);

(7) details of any initial action taken or planned in response to the relevant incident;

(8) the geographical area affected by the relevant incident;

(9) the anticipated recovery time for each *material service* affected; and

(10) any other information that will enable the *firms* and the *Regulators* to make an initial assessment of the relevant incident's potential impact.

8.3 Subject to 8.8, a *Critical Third Party*, in so far as it is aware at the time of submission of a notification under this rule, in addition to the information in 8.2, must also provide the following information to the *Regulators* about the relevant incident:

(1) the names and number of *firms* affected;

(2) where *assets* relating or belonging to *firms* have as a result of the relevant incident been lost, compromised, corrupted or become unavailable for a significant period, details of such matters;

(3) contact details of an individual (who may or may not be the individual in 4.2(1) or 8.2(4)) who is responsible for communicating with the *Regulators* about the relevant incident;

(4) details of any other regulatory body or authorities (other than the *Regulators*) that have been notified of the relevant incident; and

(5) any other relevant information about the potential impact of the relevant incident on the stability of, or confidence in, the *UK's* financial system.

8.4 The notifications under 8.2 and 8.3 must be made without undue delay after a *Critical Third Party* is aware that the relevant incident has occurred.

Intermediate Notifications

8.5 Subject to 8.8, a *Critical Third Party*, in so far as it is aware at the relevant time, must keep the *Regulators* and the *firms* to which it provides the affected services periodically appraised by providing them with the following information in relation to the relevant incident:

(1) suitable technical information that assists in understanding the nature of the relevant incident;

(2) steps taken to restore the services or recover the *assets*;

(3) information about the *Critical Third Party's* stakeholder engagement;

(4) information about any ongoing investigation;

(5) in relation to cyber-attacks:

(a) the type of threat actor (including known capabilities and motives); and

(b) the complexity and novelty of the attack;

(6) the potential impact of mainstream and social media coverage on the *Critical Third Party* and *firms* (including as a result of misinformation and disinformation); and

(7) any update on information previously provided to the recipient of the notice or any other information which the *Critical Third Party* reasonably considers to be relevant to the recipient of the notice.

8.6 Subject to 8.8, a *Critical Third Party*, in so far as it is aware at the time of submission of a notification under this rule, in addition to the information in 8.5, must keep the *Regulators* periodically appraised by providing them with the following information in relation to the relevant incident:

(1) any vulnerabilities that the relevant incident has exposed the *Critical Third Party*, other *Critical Third Parties,* a person who provides services to one or more *firms*, or *firms* to, or which have otherwise been revealed; and

(2) whether there is a risk of similar incidents happening at other *Critical Third Parties*, a person who provides services to one or more *firms*, or *firms* due to issues caused by the relevant incident or by factors in common with the relevant incident.

Final Notification

8.7 Subject to 8.8, within a reasonable time of the relevant incident in 8.1 being resolved, a *Critical Third Party* must provide the *Regulators* and the *firms* to which it provides the affected services, with the following information in relation to the relevant incident:

(1) a description of the root causes;

(2) 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;

(3) a description of the *Critical Third Party's* assessment of:

(a) the likelihood of recurrence of the relevant incident; and

(b) the long-term implications of the relevant incident on services the *Critical Third Party* provides to the *firms*;

(4) a description of identified areas for improvement for the *Critical Third Party* and, where relevant, the affected *firms*; and

(5) any other information the *Critical Third Party* reasonably considers to be relevant to the recipient of the notice.

8.8 Where a *Critical Third Party* is otherwise required to disclose something under this Chapter, but is subject to section 413 of *the Act,* it is not disclosable to *Regulators* but the *Critical Third Party* may choose whether or not to disclose it to *firms.*

8.9 A *Critical Third Party* must notify the *Regulators* promptly 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, and it poses a significant threat to the *Critical Third Party's*:

(a) reputation; or

(b) ability to provide any *material service*;

(2) the *Critical Third Party* 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;

(3) 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 bodies has commenced an investigation into its affairs;

(4) 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; or

(5) 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 meet any of its obligations under this Part.

8.10 A *Critical Third Party* must send notifications required under this Chapter to the *Regulators* and *firms* by electronic means.

8.11 A *Critical Third Party* must take reasonable steps to identify and obtain the necessary information to enable it to comply with the obligations in this Chapter.

9 INACCURATE, FALSE OR MISLEADING INFORMATION

9.1 A *Critical Third Party* must take all reasonable steps to ensure that all information it gives to the *Regulators* in accordance with the *CTP duties* 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.

9.2 If a *Critical Third Party* is unable to obtain the information required in 9.1, then it must inform the *Regulators* that the scope of the information provided is, or may be, limited.

9.3 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.

9.4 Subject to 9.5, the notification 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 why such information was or may have been provided; and

(3) the correct information.

9.5 If the information in 9.4(3) cannot be submitted with the notification (because it is not immediately available), it must instead be submitted as soon as possible afterwards.

10 NOMINATIONS

10.1 A *Critical Third Party* that has its head office outside the *UK* must comply with this Chapter.

10.2 A *Critical Third Party* coming within 10.1 must:

(1) nominate in writing a person who is authorised on behalf of the *Critical Third Party* to receive any *document* given by a *Regulator* under its *oversight functions*;

(2) notify the *Regulators* in writing of:

(a) the name of each nominated person authorised to receive any *document* on its behalf under (1);

(b) an address of a place in the *UK* for the service of *documents* to each nominated person; and

(c) an email address, telephone number and out of hours contact details for each nominated person; and

(3) notify the *Regulators* of any changes to the information notified under 10.2(2) as soon as reasonably practicable; and

(4) take reasonable steps to ensure that a person nominated to act in accordance with this Chapter:

(a) passes to it any *document* provided to it by the *Regulators*; and

(b) is cooperative and acts in a timely way with the *Regulators* when discharging any of their *oversight functions*.

11 COST OF SKILLED PERSONS REPORTS

11.1 This Chapter applies to every *Critical Third Party* and every *person connected with a Critical Third Party* required to pay a fee to a *Regulator* under 11.2.

11. 2 Where a *Regulator* 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 section166(3)(b) of *the Act* as applied by section 312P(5) of *the Act*; or

(2) collect or update information pursuant to section 166A(2)(b) of *the Act* as applied by section 312P(6) of *the Act*;

the fee payable by the *fee payer* will be the amount invoiced by the *skilled person*.

11.3 The date for payment by the *Critical Third Party* is 30 days from the date of each invoice from the *Regulator* to the *fee payer*.

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, including where applicable in complying with Chapter 3, 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 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; and

(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)—(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 *the Act* (Reports by skilled persons) or to collect or update information under section 166A (Appointment of skilled person to collect and update information) of *the Act* as applied by section 312P of *the Act* and take reasonable steps to ensure that its *employees* and agents also provide all reasonable assistance to that *skilled person*.

13 REFERALS TO OVERSIGHT BY THE REGULATORS OR TREASURY DESIGNATION

13.1 A *Critical Third Party* must ensure that neither it nor anyone acting on its behalf in any way indicates or implies that it 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 In no communication should a *Critical Third Party*, or anyone acting on its behalf, suggest that its 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 or subject to this Part.

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 it concerns the provision of 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*.