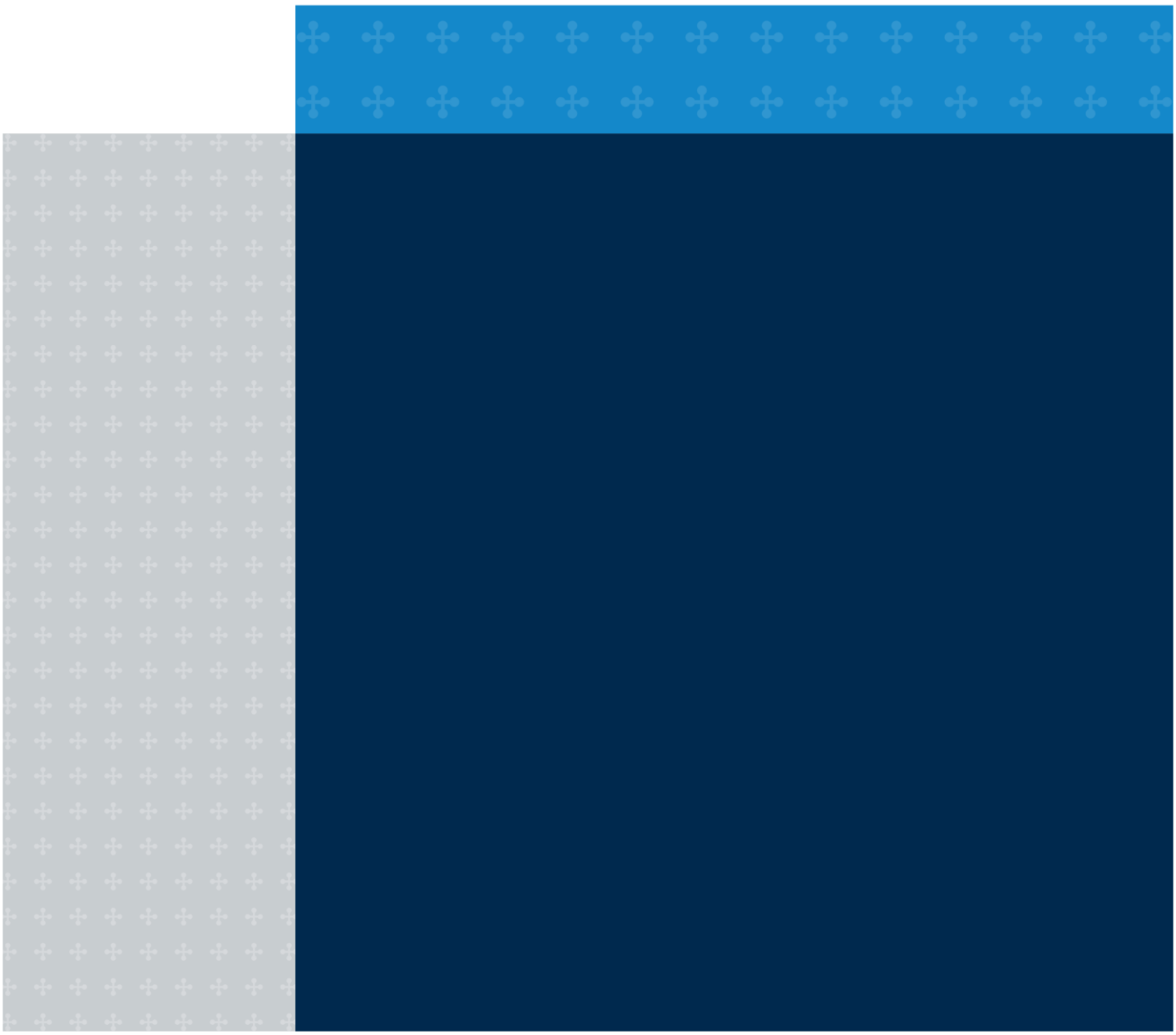
BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Publication

Policy Statement | PS7/21

Outsourcing and third party risk management

March 2021



BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Policy Statement | PS7/21

Outsourcing and third party risk management

March 2021

Prudential Regulation Authority | 20 Moorgate | London EC2R 6DA

Contents

1 Overview

1.1 This Prudential Regulation Authority (PRA) Policy Statement (PS) provides feedback to responses to Consultation Paper (CP) 30/19 'Outsourcing and third party risk management'.[1] It also contains the PRA's final Supervisory Statement (SS) 2/21 'Outsourcing and third party risk management'.

1.2 This PS is relevant to:

- banks, building societies, and PRA-designated investment firms (banks);
- insurance and reinsurance firms and groups in scope of Solvency II, including the Society of Lloyd's and managing agents (insurers);
- branches of overseas banks and insurers (third-country branches); and
- credit unions and non-directive firms.

1.3 Banks, insurers, and third-country branches are collectively referred to as 'firms' in this PS and the SS. Any parts of the PS and SS aimed at a specific subset of firms, eg insurers or third-country branches, are appropriately signposted.

1.4 Some of the contents of SS2/21 are relevant to credit unions and non-directive firms: specifically, the PRA rules, statutory powers, and requirements referenced in Tables 2, 6, and 7; and paragraphs 5.14–5.17

Background

1.5 In CP30/19, the PRA proposed to modernise its expectations relating to outsourcing and third party risk management, through an SS that would set out how the PRA expects firms to comply with the wide range of existing requirements in this area throughout the lifecycle of an arrangement. The objectives of CP30/19 were to:

- complement the PRA's policy proposals on operational resilience in CP29/19 'Operational resilience: Impact tolerances for important business services';[2]
- facilitate greater resilience and adoption of the cloud and other new technologies as set out in the Bank of England's (the Bank) response to the 'Future of Finance' report;[3]
- implement the European Banking Authority (EBA) 'Guidelines on outsourcing arrangements' (EBA Outsourcing GL);[4] and
- take into account the, at the time, draft European Insurance and Occupational Pensions Authority (EIOPA) 'Guidelines on outsourcing to cloud service providers' (EIOPA Cloud GL)[5]

1 December 2019: https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management.
2 July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.
3 https://www.bankofengland.co.uk/research/future-finance.
4 After EU withdrawal from the EU, the PRA has on-shored these GLs and they can be viewed here: Dec 2020: https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/december/gl-outsourcing-arrangements.pdf.
5 https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en.

and relevant sections of the EBA 'Guidelines on ICT and security risk management' (EBA ICT GL).[6]

Summary of responses

1.6 The PRA received 37 responses from a range of stakeholders, from PRA-regulated firms to third party service providers. There was general support for the proposals. Respondents welcomed the PRA's efforts to clarify and modernise regulatory expectations in an area where regulation had not kept pace with technological change. Firms also appreciated that the proposals complemented the PRA's policy proposals on operational resilience, given the many synergies between the two areas. Respondents noted that the proposed operational resilience framework provided a helpful lens for firms to assess how they should monitor their outsourcing and third party arrangements and establish end-to-end resilience for their important business services. Overall, responses focussed on specific areas rather than calling for a wholesale revision of the overall policy.

Changes to draft policy

1.7 Having considered the responses to the CP, the PRA has made targeted revisions to the final policy. A summary of the key changes is set out below, grouped by the relevant chapter in the SS:

SS Chapter 2: Definitions and scope

1.8 The CP proposed that arrangements performed or provided in a prudential context should be presumed to fall within the definition of 'outsourcing' in the PRA Rulebook. The final SS does not include this expectation, but instead sets out that firms should assess the materiality and risks of all third party arrangements using all relevant criteria in Chapter 5 of the SS, irrespective of whether they fall within the definition of outsourcing.

1.9 Where non-outsourcing, third party arrangements are deemed to be material or high risk, the PRA expects firms to implement effective, risk-based controls. These do not have to be the same as those that apply to outsourcing arrangements, but should be equally robust and commensurate to the materiality or risk exposure of the arrangement. There are also several PRA requirements, including the Fundamental Rules and the new requirements in the Operational Resilience Part of the PRA Rulebook, which apply to and govern the management of all third party arrangements irrespective of whether they fall under the definition of outsourcing. These requirements are listed in paragraph 2.7 of the SS.

SS Chapter 3: Proportionality

1.10 The PRA has included additional examples of how proportionality can apply to intragroup arrangements and third-country branches. These amendments do not change the PRA's position that intragroup arrangements should not be treated as inherently less risky than arrangements with third parties outside a firm's group, although certain aspects can be managed differently in practice.

SS Chapter 4: Governance and record-keeping

1.11 The PRA is planning a follow-up consultation setting out detailed proposals for an online portal on which all firms would need to submit information on their outsourcing and third party arrangements.

1.12 In the meantime, firms should continue to follow existing, relevant record-keeping requirements and expectations on outsourcing. Accordingly, banks should keep a register of all their outsourcing arrangements in line with the expectations in the EBA Guidelines, and insurers should keep appropriate records of their outsourcing arrangements. The PRA considers that a firm, in complying with 2.3(1)(e) of the Notifications Part of the rulebook, would likely already have records

6 https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/december/guidelines-on-ict-and-security-risk-management.pdf.

of its material outsourcing arrangements for this purpose. The proposed consultation on the online portal will explore how to integrate and streamline these notifications.

SS Chapter 5: Pre-Outsourcing phase

1.13 The PRA has clarified in paragraph 5.5 of the SS that if a firm outsources a service within the scope of operational continuity in resolution (OCIR) requirements, this arrangement will generally constitute 'material outsourcing'. However, the term 'material outsourcing' is broader and may also encompass outsourcing arrangements that are not within the scope of OCIR requirements but could impact a firm's safety and soundness in a going concern scenario. For instance, arrangements involving confidential, personal or sensitive data or with potential high reputational risk.

1.14 The PRA has clarified that in some circumstances, it might be appropriate for firms to notify the regulator of a planned material arrangement before a final service provider has been selected.

1.15 The SS has been updated to note that although Notifications 2.3(1)(e) as currently written only applies to material outsourcing arrangements, material non-outsourcing third party arrangements may constitute 'information of which the PRA would reasonably expect notice' within the meaning of Fundamental Rule 7 and Senior Manager Conduct Rule 4. Consequently, the PRA expects firms to bring these arrangements to its attention in a similar manner and timeframe as they would a material outsourcing arrangement.

SS Chapter 6: Outsourcing agreements

1.16 The PRA recognises that a firm may need to secure specific contractual arrangements with its third party service providers in order to meet its regulatory obligations. Therefore, an expectation has been added in paragraph 6.5 of the SS that sets out that if a third party service provider in a material outsourcing (or other third party) arrangement is unable or unwilling to include certain terms within the contract which reflect the firm's obligations under the regime, that firm should make the PRA aware of this issue.

SS Chapter 7: Data security

1.17 This chapter has been revised to take into account certain expectations set out in the EBA ICT GL. In line with the approach in the GL, this chapter applies to all outsourcing and third party arrangements, as data security can be a highly relevant consideration in non-outsourcing, third party arrangements.

1.18 After considering responses to the CP, the PRA has clarified its expectations around classification and location of data, including that none of the expectations in this SS and, in particular, Chapter 7, should be interpreted as explicitly or implicitly favouring or imposing restrictive data localisation requirements. However, the PRA expects firms to adopt a risk-based approach to the location data that allows them to simultaneously leverage the operational resilience advantages of outsourced data being stored in multiple locations and manage relevant risks.

SS Chapter 8: Access, audit, and information rights

1.19 Additional guidance has been added regarding the conduct of on-site audits. In particular, where an on-site audit could create an unmanageable risk for the environment of the provider and/or other clients, the firm and service providers should agree alternative ways to provide an equivalent level of assurance while not removing the contractual rights for an on-site audit from the written agreement. For material outsourcing arrangements, the PRA would expect the firm to inform their supervisor if alternative means of assurance have been agreed.

SS Chapter 9: Sub-outsourcing

1.20 This chapter has been revised to clarify that that the expectations in it only apply to material sub-outsourcing and that firms' primary responsibility is to ensure that third party service providers appropriately manage any material sub-outsourcing. The PRA does not expect firms to directly monitor fourth parties in all circumstances. However, when entering into a material outsourcing agreement, firms should consider the potential impact of large, complex sub-outsourcing chains on their operational resilience.

SS Chapter 10: Business continuity and exit plans

1.21 This chapter has been amended to clarify that before a contractual agreement becomes effective, firms should evaluate what would be involved in delivering an effective stressed exit and use this to formulate their exit plan.

1.22 Additional guidance has been added concerning resilience options for cloud arrangements. For instance, the PRA has clarified that there is no hierarchy or one-size-fits-all combination of cloud resiliency options.

1.23 Additional guidance has also been added to align this SS to the ICT GLs and the latest version of the CBEST implementation guide.

Cost benefit analysis and typographical changes

1.24 The PRA considers that the changes to the draft policy will not have a significant impact on firms, and will not have a significantly different impact on mutuals than for other firms. As a result, the cost benefit analysis has not been updated in respect of these changes.

1.25 The PRA has also taken the opportunity to make some typographical changes to the SS to improve readability.

Implementation and next steps

1.26 Firms will be expected to comply with the expectations in the SS by Thursday 31 March 2022. This is in line with the timing of the PRA's requirements and expectations on operational resilience as set out in PS6/21 'Operational resilience: Impact tolerances for important business services', which has been published simultaneously with this PS.[7]

1.27 Outsourcing arrangements entered into on or after Wednesday 31 March 2021 should meet the expectations in the SS by Thursday 31 March 2022. Firms should seek to review and update legacy outsourcing agreements entered into before Wednesday 31 March 2021 at the first appropriate contractual renewal or revision point to meet the expectations in the SS as soon as possible on or after Thursday 31 March 2022.

1.28 For the avoidance of doubt, the PRA considers that it is no longer proportionate for firms to make every effort to comply with the indicative timeline and process for reviewing their material (ie critical or important) legacy outsourcing arrangements as set out in paragraphs 15 and 16 of the EBA Outsourcing GL. Likewise, firms are not expected to inform the PRA if they have not met the timeline set out in the EBA Outsourcing GL. The PRA has made this decision due to the disruption and reprioritisation caused by the COVID-19 pandemic and changes to the UK, EU, and global regulatory landscape in this area (some of which are still under development at the time of publication), and in consideration of responses to CP30/19.

---

7 March 2021: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.

1.29 Firms should note that the PRA is planning a follow-up consultation setting out detailed proposals for an online portal that all firms would need to populate with certain information on their outsourcing and third party arrangements, or a subset thereof, such as those deemed material (as noted above). This consultation will take into account the comments provided by respondents to CP30/19 on the idea of developing an online portal. The PRA also plans to undertake further analysis on whether additional policy measures to manage the risks that critical third parties could pose to their objectives might be appropriate. Subject to the outcome of this analysis, the PRA may engage with industry and other relevant external stakeholders in due course.

1.30 The policy set out in this PS has been designed in the context of the UK having left the European Union and the transition period having come to an end. Unless otherwise stated, any references to EU or EU derived legislation refer to the version of that legislation which forms part of retained EU law.[8] The PRA will keep the policy under review to assess whether any changes would be required due to changes in the UK regulatory framework.

8 For further information, please see https://www.bankofengland.co.uk/eu-withdrawal/transitioning-to-post-exit-rules-and-standards.

2 Summary and general comments

2.1 The PRA must consider representations that are made to it in accordance with its duty to consult on its general policies and practices and must publish, in such manner as it thinks fit, responses to the representations.

2.2 The PRA has considered the responses received to the CP. This chapter, and those that follow, set out the PRA's feedback to those responses and its final decisions.

2.3 The chapters in this PS have been structured broadly along the same lines as the chapters of the SS. The responses have been grouped as follows:

- general comments;
- definitions and scope;
- proportionality;
- governance and record-keeping;
- pre-outsourcing phase;
- outsourcing agreements;
- data security;
- access, audit, and information rights;
- sub-outsourcing; and
- business continuity and exit plans.

General Comments

Alignment with relevant European Supervisory Authorities Guidelines

2.4 Over the last three years, all three European Supervisory Authorities (ESAs) have published guidelines and recommendations on outsourcing and third party risk management, cloud outsourcing specifically, and information and communication technology (ICT) risk management. Several standard setting bodies, such as the Financial Stability Board, have also issued policy publications on this topic. One aim of CP30/19, which was published in December 2019 when the United Kingdom (UK) was still an EU Member State, was to propose how firms should approach the EBA Outsourcing GLs and the draft EIOPA Cloud GL in light of the PRA's objectives and policy proposals on operational resilience and other unique features of the UK's regulatory regime, such as the Senior Managers and Certification Regime (SM&CR).

2.5 Twelve respondents commented on the relationship between the PRA's proposals and these ESA Guidelines. In particular, respondents encouraged the PRA to align its policy closely to the EBA Outsourcing GL and not to place additional expectations on firms. Respondents also asked the PRA to clarify the status of the final EIOPA Cloud GL on outsourcing to cloud service providers (which were published on the date of the UK's departure from the EU and came into effect the day after the end of the implementation period (Thursday 31 December 2020)), and asked the PRA not to diverge materially from them. The PRA's approach, having considered these responses, is clarified below.

2.6 In line with the approach set out in the Statement of Policy 'Interpretation of EU Guidelines and Recommendations: Bank of England and PRA approach after the UK's withdrawal from the EU'[9] the PRA no longer expects PRA-regulated firms to make every effort to comply with any ESA Guidelines that came into effect after the end of the implementation period,[10] including the following Guidelines that are relevant to the topics covered in this PS and the associated SS:

- EIOPA Cloud GL;[11]
- EIOPA ICT GL;[12] and
- ESMA Guidelines on outsourcing to cloud service providers (ESMA Cloud Guidelines).[13]

2.7 The final SS does, however, implement the:

- EBA Outsourcing GL; and
- parts of the EBA ICT GL relevant to the management of ICT third-party risk.

2.8 The PRA considers that the expectations in the SS are not materially divergent from the EBA Outsourcing or ICT GL, and has reviewed the SS in light of responses to the CP, to ensure greater consistency with these Guidelines where this is deemed to be in line with the PRA's policy objectives.

2.9 The draft SS in CP30/19 was not intended to be a line-by-line transposition of the EBA Outsourcing GL. Where the PRA has considered it justified to elaborate on the EBA's Outsourcing GL to advance its objectives, it has done so. Consequently, certain chapters in the SS provide additional guidance on key topics covered in the EBA Outsourcing and ICT GL. Examples of this include Chapters 7 (Data security) and 10 (Business continuity and exit plans). This additional guidance complements and strengthens the PRA's policy on operational resilience, and applies lessons learnt by the PRA in its supervision and enforcement of firms' outsourcing and other third party arrangements to date. Where the PRA's expectations are more granular than equivalent sections in the EBA Outsourcing or ICT GL, the PRA considers that this results in clearer, more consistent policy that will provide firms with greater regulatory certainty. As requested by several respondents, the final SS also provides more detailed guidance than the EBA Outsourcing GL on the application of proportionality to intragroup outsourcing and outsourcing arrangements for third-country branches.

2.10 The SS should be the primary source of reference for UK firms when interpreting and complying with PRA requirements on outsourcing and third party risk management. However, all relevant ESA Guidelines continue to apply to the European operations of UK firms and to the activities undertaken in the EU by firms that also have a UK presence.

Granularity of expectations compared to the policy proposals on operational resilience

2.11 Seven respondents commented on the granularity of the proposals in the draft SS, particularly when compared to the approach of CP29/19 on operational resilience. Respondents requested that

---

9 December 2020: https://www.bankofengland.co.uk/paper/2019/interpretation-of-eu-guidelines-and-recommendations-boe-and-pra-approach-sop.

10 As stated in the Statement of Policy, the Bank and PRA will consider their approach to non-legislative EU material, and may choose to issue further statements in relation to them.

11 https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/final_report_on_public_consultation_19-270-on-guidelines_on_outsourcing_to_cloud_service_providers.pdf.

12 https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-bos-20-600-guidelines-ict-security-and-governance.pdf.

13 https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf.

the SS take a more high-level, principles-based approach. Conversely, one respondent noted that they welcomed the more granular expectations.

2.12 Having considered that one response requested additional granularity while others expressed a preference for a more high-level approach, the PRA has decided to publish the final policy as proposed. This is because the SS builds on and modernises, in part, longstanding regulatory requirements and expectations on outsourcing and third party risk management (as set out in Table 1 of the SS) that were already detailed before the PRA published CP29/19 and CP30/19. In contrast, the proposals in CP29/19 sought to introduce a holistic, principles-based framework for firms to improve their operational resilience. This holistic framework brings together existing areas of regulation, such as business continuity planning, operational risk management, and outsourcing and third party risk management, all of which contain more detailed requirements and expectations.

Alignment with the Financial Conduct Authority

2.13 Two respondents commented that the policy proposals set out in CP30/19 were not aligned to the Financial Conduct Authority's (FCA) approach. The PRA coordinated and engaged with the FCA closely before and during the consultation period for CP30/19, when determining the final policy as well as when participating in relevant discussions at standard setting bodies such as the Financial Stability Board and the International Organization of Securities Commissions. The PRA considers that the expectations in the SS are compatible with the FCA's rules and guidance on outsourcing and third party risk management, although the FCA has its own specific objectives, which may sometimes lead to a different focus. The PRA and FCA's rules and expectations on outsourcing largely mirror each other. The PRA's rules and expectations are listed in Tables 1 and 2 of the SS. The FCA's rules and expectations are set out in the Systems and Controls (SYSC) Sourcebook of the FCA Handbook (in particular SYSC8 (banks) and SYSC13.9 (insurers)), as well as in FCA 'Finalised Guidance (FG) 16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services', where applicable.[14] Further information on the FCA's approach is also set out on the FCA website.[15]

Cost benefit analysis

2.14 Five respondents commented on the cost benefit analysis (CBA) in CP30/19. Two respondents noted that the more the proposals diverged from the EBA Outsourcing GL, the greater the compliance cost for firms. Two respondents noted that if the PRA took a proportionate approach to implementation, insurers would be able to rely on work that they had previously done, which would reduce costs considerably. One respondent suggested that meeting expectations around access, audit and information rights, and business continuity and exit planning could be expensive. One respondent commented that the PRA could reduce the cost for firms by only setting expectations on arrangements that support important business services. Finally, one respondent commented that it could be expensive to remediate existing contracts (referred to as legacy outsourcing arrangements in CP30/19) if the SS diverges from the EBA Outsourcing GL.

2.15 In addressing the responses relating to the cost of reviewing legacy outsourcing agreements and bringing them in line with the expectations in the final SS, the PRA has devised a more proportionate, revised implementation timeline, set out in paragraph 1.28, in order to minimise disruption and costs.

2.16 The PRA has decided not to make any further changes to the SS due to the rest of the responses related to the CBA. As noted above, the PRA considers that the SS does not diverge materially from the EBA Outsourcing GL and, where it does, it seeks to provide greater regulatory certainty in key, complex areas. The SS also complements, strengthens, and clarifies certain aspects

14 https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it.
15 https://www.fca.org.uk/firms/outsourcing-and-operational-resilience.

of the PRA's policy on operational resilience, which had a separate CBA in CP29/19 and the OCIR policy proposals, as set out in CP20/20 'Operational continuity in resolution: Updates to the policy'.[16] Finally, the SS clarifies, develops, and modernises requirements that have been in existing legislation for several years, including relevant Commission Delegated Regulations as they form part of retained EU law.

16 October 2020: https://www.bankofengland.co.uk/prudential-regulation/publication/2020/operational-continuity-in-resolution.

3 Definitions and Scope

Outsourcing and third party risk

3.1 The CP proposed that firms should assume that activities, functions, and services performed or provided by third parties in a prudential context as defined in the PRA Rulebook fall within the definition of outsourcing, and apply the remaining expectations in the draft SS to them. The CP also reiterated that third party arrangements falling outside the definition of outsourcing may not be subject to the PRA's granular, specific requirements on outsourcing. However, they are still subject to the PRA's Fundamental Rules and other existing PRA requirements and expectations, particularly relating to governance, risk management, and systems and controls. Third party arrangements are also subject to a number of relevant requirements on operational resilience, as set out in Chapter 2 of the SS. These proposals sought to prevent firms from asserting that they did not have to implement appropriate controls in relation to certain arrangements with third parties which they deemed to fall outside the definition of outsourcing in the PRA Rulebook, but which significantly impact the PRA's objectives.

3.2 There was a significant level of response to these proposals. Twelve respondents expressed concern that the PRA had blurred the distinction between outsourcing and other third party arrangements, which they stated they found confusing. Seven out of the twelve respondents commented that to presume that all arrangements performed in a prudential context should be considered outsourcing would lead to firms reclassifying a large number of third party arrangements, which would be unduly onerous.

3.3 Some respondents were concerned about the possibility of having to reclassify certain arrangements with third parties that are already subject to specific regulatory requirements as outsourcing arrangements. Examples of this include clearing, collateral management, custody, depository services, and certain market services provided by the Society of Lloyd's for London Market insurers. These arrangements are already regulated which, in the view of these respondents, already provides appropriate controls.[17] Respondents also noted that it would not be possible to comply with certain expectations in the SS in respect of these arrangements, such as those relating to exit planning.

3.4 Respondents also requested that the PRA align its approach to the EBA Outsourcing GL in the following ways:

- one respondent requested that the SS make reference to the list of arrangements that are not defined as outsourcing in the EBA Outsourcing GL;
- three respondents requested that the SS include the expectation that when considering whether an arrangement with a third party falls within the definition of outsourcing, firms should consider whether the third party will perform the relevant function or service (or part thereof) on a recurrent or an ongoing basis;
- six respondents requested that the PRA remove the reference to material outsourcing and use the MiFID II and Solvency II terminology of 'critical or important' outsourcing; and
- seven respondents requested practical guidance from the PRA on how to manage the risks in non-outsourcing third party arrangements, including the addition of extra examples. Meanwhile, three respondents expressed a preference for the PRA to take a more holistic

17 Examples of the existing regulation include Alternative Investment Fund Managers Directive, Central Securities Depositories Regulation, the FCA's CASS Sourcebook and Undertakings for the Collective Investment in Transferable Securities.

approach and revise the definition of outsourcing so that it captures relevant third party risks.

3.5 The PRA has considered these responses and has amended Chapter 2 of the SS by:

- removing the expectation that arrangements performed or provided in a prudential context fall within the definition of outsourcing. Paragraph 2.1 of the SS notes that firms should continue using the existing PRA Rulebook definition, which derives from Article 2(3) of the Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II as it forms part of retained EU law (MODR) and Article 13(28) of Solvency II. Firms will therefore not have to reclassify certain third party arrangements as outsourcing;

- in paragraph 2.4 of the SS, explicitly referring firms to the list of arrangements in the EBA Outsourcing GL that fall outside the definition of outsourcing;

- amending paragraph 2.4 to include the expectation in the EBA Outsourcing GL that when determining whether an arrangement with a third party falls within the definition of outsourcing, firms should consider whether the third party will perform the relevant function or service (or part thereof) on a recurrent or an ongoing basis; and

- clarifying that the term 'material outsourcing arrangement' should be interpreted as encompassing arrangements considered 'critical or important outsourcing' under the relevant onshored EU legislation.

3.6 Following the responses requesting greater clarity on how firms should treat third party arrangements, the PRA maintains that certain non-outsourcing third party arrangements might be highly relevant to the PRA's objectives; for instance, if they support the provision of important business services. Therefore, the SS sets out the expectation that firms should assess the materiality and risks of all third party arrangements using all relevant criteria in Chapter 5 of the SS, irrespective of whether they fall within the definition of outsourcing. Firms should attach greater importance to the dependencies and risks that their outsourcing and third party arrangements create than to specific definitions. This is sometimes referred to as 'dependency management'.

3.7 Where non-outsourcing third party arrangements are deemed to be material or high risk, the PRA expects firms to implement effective, risk-based controls. These do not have to be the same as those that apply to outsourcing arrangements but should be equally robust.

3.8 The PRA considers that its revised approach is proportionate and risk-based. Removing the prudential context presumption will promote clarity and reduce the number of arrangements that would otherwise be classed as outsourcing under the initial proposals. At the same time, the PRA's approached to material or high risk non-outsourcing third party arrangements will ensure that these arrangements are subject to appropriate, risk-based controls and do not fall into a regulatory vacuum due to an issue with their definition. It will also close any gaps that could lead to regulatory arbitrage or the application of inadequate controls to material, non-outsourcing third party arrangements.

3.9 After considering responses to the CP, the PRA has decided not to change the established definition of material outsourcing. The SS clarifies that material outsourcing encompasses any arrangements that would be deemed the outsourcing of a 'critical or important operational function' in applicable EU law. The criteria that firms should take into account to identify material outsourcing arrangements are substantively aligned to the criteria for identifying 'critical or important outsourcing arrangements' under relevant legislation (eg the EBA Outsourcing GL) with a few

justified exceptions, such as those that refer to the PRA's operational resilience requirements (see Chapter 5 in the SS).

Cloud

3.10 CP30/19 proposed that firms should assess whether an arrangement with a cloud service provider falls within the definition of 'outsourcing'. Seven respondents commented on this point and asked for further guidance, including additional examples of arrangements that the PRA would and would not consider to be cloud outsourcing. Some respondents requested clarity on whether the PRA considers that all arrangements involving the use of cloud technology, including Software as a Service (SaaS), should be defined as 'outsourcing'.

3.11 Having considered these responses, the PRA has not made any changes. To ensure a consistent approach across PRA-regulated firms, the expectations in this SS apply to all forms of outsourcing and, where indicated, other non-outsourcing third party arrangements entered into by banks and insurers. As such, cloud arrangements should not automatically be considered outsourcing. Firms should use the criteria in Chapter 2 of the SS when determining whether an arrangement is either outsourcing or a material third party arrangement. Moreover, as highlighted in paragraphs 3.7-3.8 above, the PRA's primary focus when it comes to cloud (and all other) arrangements between firms and third-parties is whether they are material or high risk rather than whether the fall into the definition of 'outsourcing'. Accordingly, if a SaaS arrangement supports an important business function, it should be subject to controls that are commensurate to its materiality, even if the firm(s) relying on it do not consider it to constitute 'outsourcing' under the definition in the PRA Rulebook.

3.12 As noted in paragraph 3.6, the PRA has included a reference to the fact that when determining whether an arrangement is outsourcing, firms should consider whether it is a one-off or a recurrent service. This means that one-off purchases, such as software licenses, should not be considered outsourcing. The purchase of a software license should, however, be considered a third party arrangement, which the PRA expects to be subject to appropriate risk based controls. It is also important to note that software purchases often rely on underlying cloud infrastructure. To manage their concentration risk, as set out in Chapter 5 of the SS, firms should take into account the effect of any indirect dependencies that may stem from software purchases.

Sub-Outsourcing

3.13 In CP30/19 the PRA set out a proposed definition of sub-outsourcing. Two respondents requested that the PRA provide further clarity on this definition. The PRA has decided not to make any changes as a result, as sub-outsourcing was clearly defined in paragraph 9.1 of the draft SS and in the PRA Rulebook. The definition of 'outsourcing' in the PRA Rulebook also explicitly acknowledges that a service provider may perform 'a process, a service or an activity which would otherwise be undertaken by the firm itself … directly or by sub-outsourcing'. The PRA considers that these definitions are sufficiently clear.

Application at legal entity level

3.14 One respondent requested that the PRA clarify the use of the term 'firm' throughout the SS. The respondent suggested that the expectations in the SS could be applied at the level of the group rather than at that of the legal entity. The PRA has considered this response and decided not to make any changes. The CP stated that its proposed expectations were designed to apply at the firm level, which is consistent with the scope of existing requirements in the PRA Rulebook and relevant legislation. The final SS clarifies the PRA's expectations on intragroup arrangements, including on the application of proportionality, more extensively than the EBA Outsourcing GL and relevant international standards.

Application to third-country branches

3.15 Two responses requested clarity on the application of the proposals to UK branches of third-country firms (third-country branches) and subsidiaries that are part of international groups. The respondents noted that regulation and terminology differs between jurisdictions.

3.16 As stated in the CP, the SS is relevant to all PRA-regulated firms, including subsidiaries and third-country branches, with proportionality applying to certain types of firm where appropriate. Outsourcing arrangements by third-country branches have been subject to the requirements in Chapter 7 of the Internal Governance of Third Country Branches (banks) and Chapter 7 of the Conditions Governing Business (insurers) Parts of the PRA Rulebook.

3.17 Since Friday 1 January 2021, the parts of the PRA Rulebook referred to in paragraph 3.15 of the SS apply to UK branches of European Economic Area (EEA) firms that were previously operating in the UK under passporting. These requirements are binding from the moment the PRA authorises these entities as third-country branches, subject to any applicable provisional exemptions for any EEA firms that enter the Temporary Permissions Regime.

3.18 While the EBA Outsourcing GL does not treat the provision of services by EU firms to their branches in the EEA as outsourcing, the PRA considers that its application of outsourcing rules and expectations to all third-country branches is justified by the:

- paramount importance of effective risk management and controls in all third-country branches deemed to be systemic, due to their potential impact on financial stability in the UK (systemic wholesale branches) as highlighted in CP2/21 'International banks: The PRA's approach to branch and subsidiary supervision';[18] and

- need to treat all UK branches of overseas firms operating in the UK consistently following the UK's departure from the EU.

3.19 The PRA recognises that third-country branches may apply certain expectations in the SS proportionately and has provided practical examples of how they may do so in Chapter 3 of the SS.

18 January 2021: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/january/international-banks-branch-and-subsidiary-supervision.

4 Proportionality

4.1 Chapter 3 of the draft SS provided guidance on the application of proportionality to the PRA's proposed expectations, particularly in relation to intragroup outsourcing and to non-significant firms, defined as those in categories 3 and below. It was also noted that 'proportionality' is a separate but complementary concept to 'materiality', which is examined in Chapter 5 of the SS. Proportionality focuses on the characteristics of a firm, including its systemic significance; 'materiality' assesses the potential impact of a given outsourcing or third party arrangement on a firm's safety and soundness, including its operational resilience.

Proportionality and materiality

4.2 There was a significant number of responses to this chapter. Seven respondents commented that it would be better to apply proportionality based on the impact of the outsourcing arrangement on the firm. Respondents requested that the PRA align to the EBA Outsourcing GL by referencing that, among other criteria, firms should consider the materiality of arrangements when determining how to apply the proposals proportionately. One respondent noted that proportionality could be applied based on the systemic significance of the outsourcing service provider. One respondent asked whether the firm was responsible for determining its own systemic significance.

4.3 Proportionality is a well-established concept in regulation. The purpose of proportionality is to ensure that the burden imposed is no greater than necessary to achieve the policy aim, taking into account the threat to the PRA's objectives. Proportionality takes into account the firm's category, internal organisation, and the nature, scope, and complexity of its activities. Paragraph 3.2 of the draft SS set out a number of factors for firms to consider when determining whether it would be appropriate to apply the requirements proportionately, and those factors have not been amended in the final version. Materiality, meanwhile, is an assessment of the importance of an outsourcing arrangement; it looks at how significant outsourcing and third party arrangements are for a given firm.

4.4 The PRA recognises that the concepts of proportionality and materiality have some commonalities. Both will inform how firms apply the expectations in the SS, and how the PRA will exercise its supervisory judgment in accordance with its objectives. To address this point and to ensure greater alignment with the EBA Outsourcing GL, the PRA has amended paragraph 3.1 of the SS to reference that firms should consider the materiality of the outsourced function when determining how to apply proportionality.

4.5 Finally, the PRA considers that it would be inappropriate to apply proportionality at the level of the service provider. Third parties may offer a combination of material and non-material services to firms and even a third party that is considered small based on metrics such as size, turnover, etc., may offer material services, such as niche technology services. Consequently, firms should focus primarily on the materiality and risks of a specific outsourced or third party service, even though the significance of the provider offering that service may be a factor in their assessment.

Proportionality for small firms

4.6 Two respondents requested greater clarity and more examples on the application of proportionality for small firms. They noted that smaller firms might outsource more functions, which would make the expectations in the SS particularly onerous.

4.7 The PRA has considered these responses and decided not to amend the final policy. The draft SS already included several examples of how smaller firms could meets its expectations proportionately. Moreover, many of the expectations in the SS (eg on access and audit rights) are

inherently proportionate and outcomes-focussed and can therefore be adapted according to the size and complexity of different firms. Further proposals on the approach that new and growing banks should follow in relation to their outsourcing arrangements were set out in CP9/20 'Non-systemic UK banks: The Prudential Regulation Authority's approach to new and growing banks'.[19]

Intragroup and third-country branch proportionality

4.8 Eight respondents commented on how to apply proportionality in an intragroup context. Respondents noted that it was particularly important for groups to understand whether they could rely on group policies, procedures, and controls for intragroup arrangements. Three respondents requested that the PRA acknowledge that the concept of 'control and influence' in relation to an intragroup agreement is broader than whether a group firm is a controlling or sole shareholder. Two firms asked for further guidance on the application of proportionality to third country branches (see also Chapter 3 above). One respondent requested that the PRA provide more details on complicated arrangements that have both intragroup and external components.

4.9 The PRA acknowledges that shareholding is not the only significant factor regarding control and influence. As a result, paragraph 3.5 of the SS has been expanded to note that, among other factors, governance structures, the allocation of senior management responsibilities (including under the SM&CR), and group-wide policies and controls may all be taken into account when assessing control and influence for the purposes of intragroup outsourcing arrangements.

4.10 Furthermore, Chapter 3 of the SS has been amended to include:

- additional examples of how proportionality may apply in intragroup situations; and
- minimum expectations that third-country branches should meet in respect of their outsourcing and third party arrangements. These expectations are balanced by the acknowledgement that in some areas, such as due diligence and exit planning, third-country branches can rely on whole firm or group policies and procedures as long as they meet their UK regulatory obligations. For an explanation regarding the application of outsourcing rules and expectations on third-country branches, see Chapter 3 above.

Miscellaneous comments

4.11 One respondent requested that the PRA provide examples of how the expectations could be applied proportionately throughout the SS. Two respondents requested that the PRA provide more examples of how proportionality could apply to general insurers, which they believed pose a lower threat to financial stability. One respondent noted that the FCA does not support proportionality for intragroup arrangements.

4.12 Having considered these responses, the PRA has decided to publish the policy as proposed. The PRA does not consider that general insurers automatically pose a lower threat to financial stability than other types of firm. In addition, the PRA has a specific statutory objective to contribute to securing an appropriate degree of protection for those who are or may become policyholders. This objective strengthens the argument for promoting a consistent set of requirements and expectations for banks and insurers in respect of their outsourcing and third party arrangements. Moreover, as the examples in Chapter 3 of the SS apply equally to banks and insurers, the PRA does not consider it necessary to provide specific examples of how proportionality may apply to insurers.

---

19 July 2020: https://www.bankofengland.co.uk/prudential-regulation/publication/2020/new-and-growing-banks.

5 Governance and record keeping

5.1 The CP proposed expectations regarding:

- board engagement on outsourcing;
- the requirement for firms to meet the Threshold Conditions at all times and avoid becoming 'empty shells';
- the application of the SM&CR to outsourcing. This includes the prescribed responsibilities in Rule 4.1(21) in the Allocation of Responsibilities Part of the PRA Rulebook (banks), and Rule 3.1 in the Insurance - Allocation of Responsibilities Part of the PRA Rulebook (insurance); and
- the contents of the outsourcing policy that banks are expected to maintain under the EBA Outsourcing GL and EBA GL on Internal Governance, and that insurers are required to maintain under Rule 2.4(1) in the Conditions Governing Business Part of the PRA Rulebook.

Expectations for board committees

5.2 Two respondents commented on the PRA's expectations for board committees. One considered that the proposals blurred the responsibilities between senior management and the board, and that the PRA should take a more outcome-focussed approach. One respondent requested that the PRA amend the wording in paragraph 4.4 of the draft SS to make clear that boards are responsible only for identifying and understanding the firm's reliance on outsourcing providers, rather than all critical service providers.

5.3 The PRA has decided not to make changes to the final policy as a result of these responses. As set out in SS5/16 'Corporate Governance: Board responsibilities', the PRA considers that the specific accountabilities of individual directors established by the Senior Managers Regime are additional and complementary to the collective responsibility shared by directors as members of the board.[20] Paragraph 4.4 of the SS has not been amended, as it contains established principles that were published in the PRA's Final Notice against R. Raphael & Sons plc.[21]

The SM&CR and outsourcing

5.4 Four respondents commented on the application of the SM&CR to outsourcing. One respondent queried whether accountability for outsourcing could be shared among Senior Management Functions (SMFs). They also asked for more guidance on the responsibilities of the Chief Operations function (SMF24). Two respondents asked the PRA to recognise that it can be challenging for firms to ensure clear accountability for day-to-day management of outsourcing and third party risk below the SMF level. One respondent requested clarity on the interaction between the SM&CR and the PRA's policy on operational resilience.

5.5 The PRA has not made changes to the SS as a result of these responses. The PRA's expectations regarding the role of the SMF24, the allocation of the prescribed responsibility for outsourcing, and the need for clear and explicit allocation of all responsibilities relating to outsourcing and third party risk management are clear and well established, including in other SSs that firms may find useful.[22]

---

20 July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2016/corporate-governance-board-responsibilities-ss.

21 May 2019: https://www.bankofengland.co.uk/news/2019/may/fca-and-pra-jointly-fine-raphaels-bank-1-89m-for-outsourcing-failings.

22 Paragraphs 2.22A, 2.22L, 2.31, 2.33, 2.37A, 2.37B, 2.40, 2.52, 2.93 in SS35/15 'Strengthening individual accountability in insurance', August 2015: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-insurance-ss. Paragraphs 2.11-G, 2.41A in SS28/15 'Strengthening individual accountability in banking', July 2015: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss.

For clarity on the interaction between the SM&CR and the PRA's policy on operational resilience, firms should consult the final policy in PS6/21 and SS1/21.

Outsourcing policy

5.6 Five respondents commented on the PRA's expectations for the outsourcing policy that firms are expected to maintain. One respondent requested clarification that the policy does not need to be contained in a single document, and that a firm is only expected to provide a service provider with the relevant sections of the policy rather than the whole document, in particular if parts of the policy contain confidential or sensitive information. Another respondent suggested that the SS should explicitly permit firms to have different policies for external and intragroup outsourcing. This respondent also requested that institutions should be permitted to include further details on aspects of the outsourcing policy in appropriate governance documents. One respondent commented that the outsourcing policy should be more principles-based and flexible so that it does not impede the on-boarding of third party providers. One respondent requested that the PRA confirm that by sharing their outsourcing policies with service providers, firms are not diluting their own responsibilities.

5.7 Having considered these responses, the PRA has amended Chapter 4 of the SS to clarify that there is no one-size-fits-all template for firms' outsourcing policies, and that the outsourcing policy does not have to be contained in a single document. As stated in the draft SS, firms and groups are responsible for developing and maintaining a policy that is appropriate to their complexity, organisational structure, and size. It may therefore be appropriate, for example, for firms to have separate policies for their intragroup and external outsourcing arrangements as long as all of the information in Table 4 in the SS is appropriately captured.

5.8 Paragraph 4.11 has been revised to clarify that, where relevant, firms should make outsourced and third party providers aware of the relevant parts of their internal policy, but can omit or redact confidential sections thereof. The PRA has also amended the same paragraph to clarify that sharing these policies with third party service providers does not dilute firms' responsibilities in terms of managing their outsourcing and third party arrangements, but can help third party service providers get a better understanding of firms' regulatory obligations and other relevant aspects such as their risk tolerance and expected service levels.

Empty shells and Threshold Conditions

5.9 One respondent noted that they would welcome further guidance on the criteria for how to avoid becoming empty shells that are incapable of meeting the Threshold Conditions. The PRA considers that the guidance provided in paragraph 4.6 of the SS is sufficient. Further guidance on the PRA's approach to the Threshold Conditions is set out in paragraph 21 of 'The PRA's approach to banking supervision' and paragraph 25 of 'The PRA's approach to insurance supervision'.[23]

Internal record keeping requirements

5.10 The CP proposed that all PRA-regulated firms should maintain an internal register of their outsourcing agreements in line with the EBA Outsourcing GL. It included an annex to clarify and promote consistency on how firms should fill in this register. In parallel, the PRA consulted on the idea of a technological solution, in the form of an online portal where firms would submit the data in their outsourcing registers, or parts thereof, to the PRA. It was noted that the proposed portal, if it went ahead, would require further consultation to consider its design features and other aspects.

---

23 October 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/pras-approach-to-supervision-of-the-banking-and-insurance-sectors.

5.11 Twenty-two respondents commented on the internal record keeping proposals. Five respondents opposed the proposal that insurers should keep an internal register of all their outsourcing arrangements (consistent with the approach already in place for banks), which they considered would be costly and of little value to them. In addition, two respondents suggested that the PRA should publish a subsequent consultation on extending the internal record keeping requirements to insurers. Four respondents noted that the PRA should ensure that its internal record keeping expectations are proportionate and consider ways to streamline the data required. Four respondents requested clarity on how the PRA expects firms to record intragroup arrangements, particularly those that involve sub-outsourcing, and whether the register could be held at a group level. Generally, respondents urged the PRA to minimise discrepancies with the outsourcing register required under the EBA Outsourcing GL and other jurisdictions' record keeping requirements.

5.12 Respondents were generally supportive of the idea of an online portal but asked the PRA to consider carefully issues such as data security and intended use of any data collected.

5.13 The PRA has considered the extensive responses on this topic and concluded that, in the medium-term, it is essential to have access to clear, consistent data from banks and insurers about their outsourcing and third party dependencies, in order to identify, monitor, and manage systemic concentration risk. Therefore, the PRA intends to publish a subsequent consultation setting out proposals for an online portal that banks and insurers would need to populate with information on their outsourcing and third party arrangements or a subset thereof, such as those deemed material. The initial proposals in this consultation will take into account relevant responses received to CP30/19 while also providing consultees with a further opportunity to provide comments. This consultation will also include details on the design of the portal itself.

5.14 In the interim, and while the PRA consults on the proposed online portal, firms should continue to meet existing record keeping requirements and expectations. Accordingly, banks should follow the record keeping expectations in the EBA Outsourcing GL, and insurers should keep appropriate records of their outsourcing arrangements. The PRA considers that a firm, in complying with 2.3(1)(e) of the Notifications Part of the rulebook, would likely already have records of its material outsourcing arrangements for this purpose. The proposed consultation on the online portal will explore how to integrate and streamline these notifications. The PRA also expects that firms should make information on their outsourcing and third party arrangements of which the PRA would reasonably expect notice available to it in accordance with Fundamental Rule 7. The PRA may request data on firms' outsourcing arrangements under Section 165 of the Financial Services and Markets Act 2000 (FSMA), provided that the statutory tests are met, and/or through data collection exercises that the PRA may consider it reasonable to undertake.[24]

[24] The PRA may exercise, under section 165A of FSMA, the power to require certain persons to provide (i) specified information or information of a specified description; or (ii) specified documents or documents of a specified description, that it considers are, or might be, relevant to the stability of one or more aspects of the UK financial system (the financial stability information power).

6 Pre-outsourcing phase

Materiality Assessment

6.1 The CP proposed to introduce common criteria, set out in Chapter 5 of the draft SS, to improve the consistency and quality of firms' assessments of the materiality of outsourcing arrangements. In total, eight respondents commented on these proposals:

- Five respondents thought that the materiality criteria set out in the SS was too prescriptive and that firms should develop their own processes. Conversely, one respondent asked for further guidance.

- Two respondents requested that the criteria set out in Table 4 of the draft SS should be clarified to explain that the potential impact of disruption, failure, or inadequate performance should be measured by the materiality of the impact, rather than the likelihood of a specific incident occurring.

- One respondent asked the PRA to confirm whether the materiality assessment could be performed at the service level.

- Four respondents requested further examples of what would be considered a material cloud outsourcing arrangement. They also asked the PRA to clarify that the presence of cloud does not automatically make an arrangement material.

- Two respondents offered additional materiality criteria for the PRA to consider.

- One respondent noted that a service provider may provide limited services to one firm, but a much wider range of services to another firm. Therefore, they requested that the PRA acknowledge that different services provided by the same provider may be subject to different materiality assessments.

- Two respondents requested that the PRA align the wording in the materiality criteria more closely to that contained in the EBA Outsourcing GL.

- Seven respondents commented on the criteria for the reassessment of an arrangement's materiality. They noted that the requirement to reassess materiality when an arrangement is 'scaled up' should only be triggered when there is a material change in the underlying service provided or its associated risk, rather than by an organisational change at the service provider or sub-outsourced service provider (see Chapter 9 of the SS for a definition of sub-outsourcing).

- Four respondents commented on the reference in the materiality criteria to services deemed critical under OCIR. They asked whether the outsourcing of such services would automatically be considered material. It was noted the reference in the draft SS to 'OCIR and resolvability' was different to the language used in the EBA GLs. One respondent noted that the PRA's reference to OCIR and resolvability was unnecessary as this concept was compassed by the EBA's reference to the soundness or continuity of the arrangements.

6.2 After considering these responses, the PRA has decided to take some of the points into account, but not to substantially change the materiality criteria set out in Table 5 of the final SS. At present, there can be significant inconsistencies in firms' materiality assessments, criteria, methodologies and conclusions, which indicates a need for guidance to promote consistency. Moreover, while the SS

states that firms should have regard to the criteria set out in Table 5, it also includes an expectation that firms should develop their own processes for assessing materiality as part of their outsourcing policies.

6.3 The PRA has decided to make the following targeted amendments:

- clarifying that when a firm outsources a service within the scope of OCIR requirements, this arrangement will generally amount to a material outsourcing arrangement. However, the term 'material outsourcing' may also encompass outsourcing arrangements that are not necessarily critical from a resolution perspective, but could impact on the PRA's objectives in a going concern scenario;

- highlighting that the presence of cloud or any other given technology does not, in itself, automatically render an outsourcing arrangement material;

- modifying the wording around obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act to align more closely to the equivalent parts of the EBA Outsourcing Guidelines; and

- redrafting paragraph 5.8 to clarify that a materiality reassessment should take place when there has been a significant organisational change at the service provider or a material sub-outsourced service provider that could materially change the nature, scale, and complexity of the risks inherent in the outsourcing arrangement, including a significant change to the service provider's ownership or financial position.

6.4 The PRA has also confirmed that when assessing the potential impact of the disruption, failure, or inadequate performance of an outsourcing or third party arrangement, firms should take into account the likelihood of such disruption, failure, or inadequate performance.

Notifications

6.5 The CP proposed that to comply with Notifications 2.3(1)(e) and Fundamental Rule 7, the PRA would expect firms to notify it of material outsourcing arrangements sufficiently in advance of entering into them, to allow appropriate supervisory scrutiny.

6.6 One respondent commented that it would be preferable to tell firms exactly how far in advance they should notify the PRA. Another respondent noted that firms have to strike a balance between early notification, when they may not have all the necessary information, and a later notification that is more complete. One respondent requested that the PRA develop a standard notification template. One respondent asked the PRA to provide more guidance on what information the notification should contain.

6.7 The PRA considers that giving a precise, prescriptive timeline for notifications would be unduly prescriptive, lead to a one-size-fits-all approach, and constrain firms from using their judgement. The possibility of standardising how material outsourcing notifications are submitted will be considered in the consultation on the proposed portal as mentioned above. In the meantime, the SS sets out clear expectations on the minimum information expected in material outsourcing notifications while still allowing firms the flexibility to provide further information if they consider it appropriate.

6.8 One respondent requested that the PRA confirm that it does not approve outsourcing arrangements and that it does not need to wait for feedback before entering an arrangement. Regulatory permission is not part of the notification process. However, if the PRA considers that a proposed outsourcing arrangement poses risks to its objectives, it may consider actions ranging from

informal feedback to the use of statutory powers (eg Section 55M of FSMA). It is therefore essential that firms notify the PRA sufficiently early of proposed material outsourcing arrangements to allow for an appropriate assessment and discussion by supervisors.

6.9 As noted in Chapter 3 above, respondents requested greater clarity on the management of material or high risk third party arrangements. In light of these responses, the SS has been updated to note that although Notifications 2.3(1)(e) only applies to material outsourcing arrangements, material non-outsourcing third party arrangements may also constitute 'information of which the PRA would reasonably expect notice' within the meaning of Fundamental Rule 7 and Senior Manager Conduct Rule 4. Consequently, the PRA expects firms to bring these arrangements to its attention in a similar manner and timeframe as for a material outsourcing arrangement. The proposed consultation on the online portal will explore how to integrate and streamline these notifications. In the meantime, if appropriate and convenient, firms may develop and use their own internal frameworks for making these notifications.

6.10 One respondent asked for further details on the notification of intragroup arrangements and whether it would be appropriate to notify the regulator at a group level of material outsourcing arrangements. Another two respondents asked the PRA to clarify how firms should notify the PRA of any outsourcing arrangements which it may reclassify as material as a result of the criteria and expectations in the SS.

6.11 In light of these responses, Chapter 3 of the SS has been amended to include the expectation that if a UK consolidated group is entering into a material outsourcing arrangement that covers the entire group, a single notification under Notifications 2.31(e) will suffice, provided that the notification lists all the individual firms that will receive the relevant service.

6.12 The PRA has not set a fixed timeline for firms to notify it of any existing non-material arrangements which they may subsequently reclassify as material in light of the criteria in the SS. Firms may do so by submitting a single blanket notification to the PRA, such as a list in an accessible format of all arrangements reclassified as material.

Due diligence

6.13 The CP proposed expectations relating to firms' due diligence in assessing prospective service providers, and highlighted the importance of assessing the risks of all outsourcing arrangements irrespective of their materiality.

6.14 Seven respondents commented that the proposed due diligence expectations were burdensome and requested that the PRA take a more proportionate approach. It was also noted that excessive due diligence requirements could deter service providers from offering services to the financial services sector. Respondents requested further clarity on how to take a proportionate approach to the risk assessment for non-material outsourcing.

6.15 The PRA considers that appropriate due diligence and risk assessments, which are already required under MiFID II and Solvency II, are an essential part of the pre-outsourcing process, as they ensure that the firms screen prospective service providers and select the most appropriate one. However, the PRA has amended the SS to clarify that full due diligence is not required on all service providers but that firms should identify alternative providers at the pre-outsourcing stage to facilitate appropriate exit planning (see Chapter 11 below).

6.16 In response to further guidance on the due diligence process, the SS has been amended to include the expectation that firms should consider the ability of a service provider to provide the

service that the firm needs in a manner compliant with UK regulatory requirements. In addition, the PRA has clarified that if, as part of the due diligence process, a firm cannot identify an appropriate alternative or back-up provider, they should consider alternative business continuity plans, contingency plans, and disaster recovery measures to ensure that they can continue providing relevant important business within their impact tolerances in the event of material disruption at their chosen service provider.

Concentration risk

6.17 The CP proposed that firms and groups should periodically (re)assess and take reasonable steps to manage their overall reliance on third parties, as well as concentration risks or vendor lock-in at firm or group level.

6.18 Seven respondents commented on this proposal. It was noted that concentration risk is not a new phenomenon and that vendor lock-in has existed for a long time within financial services; and that there are limits to the extent that firms can manage concentration risk due to the small number of suppliers in specific areas such as cloud computing. Some respondents requested clarity on the expected outcome of managing concentration risk.

6.19 The PRA recognises that there are two separate dimensions to concentration risk. On the one hand, individual firms and groups are responsible for managing firm-level and group-level concentration risks, including multiple exposures within a firm or group to a single or small number of service providers. Unmanaged concentration risk at the firm or group level can result in unplanned service outages, operational disruption, and ineffective business continuity and exit plans.

6.20 In response to the lessons learned from Covid, the SS has been updated to note that concentration risk can also arise when a firm has a multitude of arrangements in the same geographic jurisdiction or region (eg business process outsourcing), even if these arrangements are with multiple, unconnected third parties. The SS has also been updated to note that to monitor and manage concentration risk, firms should take into account fourth party/supply chain dependencies; for instance, where multiple otherwise unconnected service providers depend on the same material sub-contractor for the delivery of their services.

6.21 As noted in the CP, there is a connected but separate challenge of concentration risk where a single service provider, or a small number of service providers which are very difficult to substitute, may provide certain outsourced and third party services to large numbers of PRA-regulated firms (hereafter ‘critical third parties’). The failure of, or a prolonged significant disruption at, a critical third party could have adverse consequences on the safety and soundness of multiple firms and, potentially, on financial stability. The CP specifically invited responses on how the potential impact of all critical third parties on financial stability could be better assessed, monitored and managed both domestically and internationally in a way that helps advance financial stability and promote the operational resilience of firms. This topic is addressed in more detail in chapter 12 of the PS.

7 Outsourcing agreements

7.1 Article 31(3) of MODR (banks) and Article 274(3)(c) of the Solvency II Delegated Regulation require all outsourcing arrangements, irrespective of materiality and including intragroup arrangements, to be set out in a written agreement. The draft SS proposed areas that the PRA would expect, as a minimum, contracts for 'material outsourcing' arrangements to address.

Alignment with the EBA Guidelines

7.2 Two respondents commented on the alignment between the PRA's expectations for outsourcing agreements and the equivalent sections of the EBA Outsourcing GL. One respondent asked the PRA to confirm that the SS does not impose any additional requirements.

7.3 The PRA considers that the differences between the expectations in the SS and the equivalent sections are largely editorial. The only substantive addition the CP proposed was that in light of the PRA's operational resilience policy, the PRA would expect the written agreement to include provisions regarding the testing of business continuity and exit plans, which should take account of firms' impact tolerances for important business services. This expectation has been retained in the final policy because without the inclusion and co-operation of outsource providers, firms will be unable to test their ability to remain within their impact tolerance during a period of operational disruption.

Burden of engaging in negotiations with suppliers

7.4 Seven respondents commented on the challenges of negotiating outsourcing agreements that meet the PRA's expectations. Respondents noted that there can be an imbalance in negotiating power between smaller firms and dominant third party service providers. One respondent commented that consequently, the PRA should have fewer, more targeted regulatory expectations.

7.5 Having considered these responses, the PRA has decided not to reduce its expectations. The minimum contractual safeguards set out in the SS are essential to ensure that key provisions in other chapters of the SS, notably access to audit and information rights, data security, and business continuity and exit plans, are rendered contractually effective. Moreover, the imbalance in contractual power between a small firm and a dominant service provider should not be considered as justification for a firm to accept clauses and terms that do not meet legal or regulatory expectations. This principle is set out in financial regulation and other areas, such as data protection law.

7.6 The PRA must so far as is reasonably possible act in a way which, as a secondary objective, facilitates effective competition in the markets for services provided by PRA-authorised persons in carrying on regulated activities. The PRA consider that while respondents have noted that there exists an imbalance in negotiating powers between smaller firms and dominant third parties, by providing greater regulatory certainty, the final policy will help to ameliorate this disparity.

7.7 However, the PRA also recognises that firms may need to secure specific contractual arrangements with its third parties in order to meet the PRA's expectations. Therefore, an expectation has been added in paragraph 6.5 of the SS that if an outsourced service provider in a proposed material outsourcing arrangement is unable or unwilling to contractually facilitate a firm's compliance with the PRA's regulatory obligations and expectations, firms should make the PRA aware.

Miscellaneous feedback

7.8 Two respondents asked whether the PRA would consider amending the expectation for the contract to include the governing law of the agreement. They noted that alternative dispute resolution or arbitration are alternative avenues for resolving disputes.

7.9 The PRA has added some wording to reflect that the expectations in Chapter 6 of the SS do not in themselves preclude the use of alternative dispute resolution mechanisms to settle contractual disputes between firms and third party service providers.

7.10 One respondent commented that the PRA should clarify whether termination rights should be required for material breaches of applicable law, regulation, or contractual provision. They indicated that they would also welcome further guidance on how to take appropriate corrective steps where necessary to terminate an agreement. The draft SS's wording on termination rights was consistent with the EBA Outsourcing GL, which expect outsourcing arrangements to expressly allow the possibility for firms to terminate the arrangement, in accordance with applicable law in a range of scenarios, including all breaches of applicable law, regulations, or contractual provisions. Some additional non-exhaustive examples of situations where a firm might consider exercising termination rights have been added to the SS. In consideration of this response, the PRA considers that, in the interest of proportionality and pragmatism, firms may want to limit contractual termination rights to situations where the breaches of law, regulation, or contractual provisions are either material, not expediently remediated, or create risks beyond a firm's tolerance.

7.11 The CP noted that the written agreement should include whether the service provider should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover requested. One respondent noted that firms should consider the use of escrow agreements. The PRA considers that an escrow agreement is one of a number of relevant resiliency options that firms may wish to consider when undertaking their business continuity and exit planning. The PRA does not mandate or favour the inclusion of any single resiliency option in outsourcing contracts but encourages firms to explore all appropriate and viable options, which may include escrow.

7.12 Two respondents noted that for intragroup agreements, a lighter touch approach to the expectations for the outsourcing agreement would be more appropriate. In response, the PRA reminds firms that Chapter 3 of the SS, on proportionality, specifically notes that written agreements may be adapted for intragroup outsourcing.

7.13 Regarding the monitoring of outsourcing agreements, two respondents noted that the use of key performance indicators should be discretionary. In response to these comments, the PRA acknowledges that there is no one-size-fits-all approach to monitoring service providers' performance. The SS has been revised to make clear that the agreement should include the right of the firm to monitor the service provider's performance on an ongoing basis. This can be achieved by reference to key performance indicators, but this is not compulsory in all circumstances.

8 Data security

8.1 The CP proposed expectations on how firms would ensure that data in material outsourcing arrangements are protected adequately.

Data Security

8.2 Seven respondents asked for further guidance on the PRA's expectations around encryption. In particular, they noted that it might be practically difficult to make encryption keys accessible to the PRA. Respondents were also concerned that some of the expectations on data security were too prescriptive. Three respondents noted that the list of security requirements in paragraph 7.10 of the draft SS were not appropriate in all situations and could prevent firms from taking a more risk-based approach.

8.3 In light of this feedback, the PRA has amended paragraph 7.11 to make clear that the controls required will depend on the materiality and risk of the outsourcing arrangement. The PRA expects these controls to include a range of preventative and detective measures. Paragraph 7.12 of the SS has also been amended to clarify that the PRA expects firms to ensure that the data protected by encryption (although not necessarily the encryption keys themselves) should be provided to the PRA in an accessible format if required in accordance with Fundamental Rule 7 and other potentially relevant regulatory requirements.

Data location

8.4 The CP proposed that firms should take a risk-based approach to data location, considering data-at-rest, data-in-use, and data-in-transit. Five respondents commented on this proposal. They queried whether it was appropriate to set expectations regarding the location of data-in-transit. One response asked the PRA to identify a list of high-risk jurisdictions to establish a uniform understanding of where legal and practical challenges may be an issue. One respondent requested that the PRA remove data location requirements for outsourcing arrangements on the public cloud as it undermines the benefits of global data centres. One respondent requested that the PRA reflect on the impact of the Court of Justice of the European Union's (CJEU) recent decision in the Schrems II case.[25]

8.5 The PRA has considered this feedback and decided to maintain the expectation that firms should know the location of their data at all times, including when in transit. To assist firms, the SS has been updated to set out that as part of the due diligence and risk assessment in the pre-outsourcing phase, firms should identify whether their data could be processed in any high risk jurisdiction(s) that are outside the risk tolerance in their outsourcing policy.

8.6 The PRA has clarified that none of the expectations in the SS and, in particular, Chapter 7, should be interpreted as explicitly or implicitly favouring or imposing restrictive data localisation requirements. However, the PRA expects firms to adopt a risk-based approach to the location data that allows them to simultaneously leverage the operational resilience advantages of outsourced data being stored in multiple locations and manage relevant risks. The PRA has also decided that it would not be appropriate for it to publish and maintain a list of high-risk locations.

8.7 In relation to the impact of the CJEU's decision regarding Schrems II, this had implications for a range of sectors including but not limited to financial services. Providing a PRA-specific view could conflict with guidance from the Information Commissioner's Office and other data protection authorities. Firms should monitor and observe requirements and guidance from relevant authorities

25 https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

and consider GDPR-compliant mechanisms for transferring data to other jurisdictions. Examples of these include standard contractual clauses and, in an intragroup context, potentially binding corporate rules.

Data classification

8.8 Seven respondents commented on the data classification expectations proposed in the SS. In particular, they queried whether it was essential to classify all the data required in the event of operational disruption. Respondents noted that as part of GDPR compliance they had already completed significant projects to appropriately classify personal data. In addition, one respondent disagreed that data migration would be a prudent course of action in the event of disruption. They asserted that it would be preferable to allow agreed incident management processes to progress and work towards resumption of services.

8.9 The PRA has considered this feedback and redrafted the data classification section of the chapter so that it is less prescriptive and more outcomes-focussed. While the PRA does not prescribe a specific data classification taxonomy, it expects firms to implement appropriate, proportionate, and risk-based technical organisation measures to protect different classes of data (eg confidential, client, personal, sensitive, or transaction). Firms' compliance with GDPR may already bring them in line with the PRA's expectations in this area. However, the PRA's objectives and expectations on operational resilience support the expectations on data classification in the SS, which may extend to confidential or sensitive non-personal data.

Miscellaneous

8.10 Two respondents asked for further clarity on how the shared responsibility model will work in practice. Three respondents also noted that providers may be reluctant to agree to customer specific security requests.

8.11 The PRA has considered these responses. The example table setting out the shared responsibility model has been moved to Chapter 4 of the SS, because the PRA expects firms to define, document, and understand their and the service provider's respective responsibilities for all outsourcing arrangements. The shared responsibility model is provided only as an illustrative example, albeit widely-used in certain types of arrangement, of how some firms may choose to meet this expectation in relation to their cloud arrangements, and is not the only option.

8.12 Regarding outsource providers' accommodation of customer-specific security requests, the PRA has not made any changes in response to this feedback. The ability of service providers to respond to customer-specific security requests may vary depending on the type of service being provided. As a general rule, the more standardised the service, the more difficult it might be for the service provider to accommodate these requests. The PRA's main focus is on the overall effectiveness of the service provider's security environment, which should allow firms to meet their regulatory and risk management obligations and be of equal or greater effectiveness than their in-house environments. As long as service providers can provide appropriate assurance that this is the case, the PRA does not have specific expectations around customer-specific requests.

9 Access, audit, and information rights

9.1 The CP noted that obtaining appropriate access, audit, and information rights is often a key challenge for firms when negotiating outsourcing agreements. The draft SS proposed a number of ways that firms could exercise these rights in a proportionate way, including pooled audit and third party certification.

Onsite audits

9.2 Seven respondents commented on the PRA's proposal that the outsourcing agreement should provide unrestricted access, audit, and information rights. Respondents noted that they would prefer the language in the SS to align to the equivalent section of the EBA Outsourcing GL. Three respondents commented on the PRA's proposed expectations for onsite audits. Several practical suggestions were made to improve the process of onsite audits for firms and service providers. One respondent requested that service providers should be able to limit the data or locations where they provide access if there are reasonable security concerns. Another response suggested that the PRA should allow firms and service providers to make alternative arrangements when the risks of an onsite visit cannot be satisfactorily managed.

9.3 The PRA has considered these points and decided to make the following amendments to the SS:

- in line with the original policy intention, the language around access, audit, and information rights has been reviewed and updated to ensure consistency with the EBA Outsourcing GL;

- the SS has been updated to note that as part of providing a service provider with reasonable notice of an onsite visit, the firm should include the location and purpose of the visit and the personnel that will participate; and

- the SS acknowledges that certain types of onsite audit create may an unmanageable risk for the environment of the provider and/or another client of the same provider, for instance by impacting the provider's service levels or the confidentiality, integrity, and availability of data. In such cases, the firm and the service provider should agree on alternative ways to provide an equivalent level of assurance. This could, for example, be achieved through the inclusion of specific controls to be tested in a report or certification. The PRA expects that firms should retain their underlying right to conduct an onsite audit. For material outsourcing arrangements, the PRA expects firms to inform their supervisor if alternative means of assurance have been agreed.

Third party certification

9.4 One respondent suggested specific drafting changes to the section on third party certification, to ensure that firms' requests for additional informational are proportionate. In response, the PRA has made minor amendments to Table 8 and paragraph 8.10 in the SS to clarify that firms should request additional, appropriate, and proportionate information if such a request is justified from a legal, regulatory, or risk management perspective.

Pooled audits

9.5 Six respondents commented on the PRA's proposals concerning pooled audits. Three respondents raised concerns that pooled audits are not a practical audit solution and may not satisfy all firms' requirements adequately. Two respondents requested that the PRA provide more examples of how pooled audits could work in practice. One respondent queried whether pooled audits would be an acceptable alternative to the negotiation of full access, audit, and information rights.

9.6 The PRA has not made any changes to the SS in response to this feedback. The PRA recognises that pooled audits may provide an appropriate, collaborative, cost effective, and proportionate method of obtaining assurance and information from common third parties. However, the PRA does not mandate pooled audits, and it is for firms to decide whether this is a suitable assurance mechanism for their outsourcing arrangements. Furthermore, if a group of firms conducts a pooled audit or relies on another collaborative method for obtaining assurance and information from common third party service providers, each firm remains individually responsible for meeting its legal and regulatory obligations.

9.7 The PRA recognises that coordinating pooled audits can entail coordination and logistical challenges, including with regard to confidentiality and scoping. However, the PRA considers that, if adequately organised and executed, they can be a valuable mechanism to assess the control environments of common third party providers. In future, the PRA would welcome the opportunity to discuss the scoping and general results of any pooled audits conducted by groups of firms, without prejudice to any confidentiality or non-disclosure requirements.

Miscellaneous feedback

9.8 One respondent requested further information on how to apply access, audit, and information rights proportionately in an intragroup context. In response to this feedback, the PRA has added additional guidance on how firms can exercise their access and audit rights proportionately in a group context.

9.9 Three respondents raised questions about whether it was permissible to involve third parties in the audit process. A clearer definition of the range of stakeholders involved in the audit process was also requested.

9.10 The PRA understands the important role that external experts appointed by a firm or group of firms, such as cyber security consultants, can play in audits of third party service providers, particularly those providing technically complex services. Paragraph 8.3 of the SS covers the role of external experts, and notes that contractual access, audit, and information rights should extend to other persons appointed by the firm. The PRA has decided not to define the range of stakeholders that can be involved in an audit of a third party service provider, as this can vary depending on the third party, the service, and the firm(s) involved, among other factors.

9.11 Regarding the regulator's access, audit, and information rights, one firm requested clarification on how the PRA will exercise these rights. Another firm requested that the PRA remove references to the regulator's rights from the written agreement. A respondent also asked if the PRA could expand on the role of the supervisory authorities in the event of disruption to national critical infrastructure.

9.12 In light of these responses, the PRA confirms that it will exercise its access, audit and information rights in line with the broader approach set out in the approach to supervision documents.[26] As such, while the PRA looks to firms to co-operate with it in resolving supervisory issues, it will not hesitate to use formal powers, including access, audit and information rights, where it considers them to be an appropriate means of achieving its desired supervisory outcomes, where the commensurate statutory tests are met, and where it constitutes a reasonable and proportionate approach.

---

26 October 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/pras-approach-to-supervision-of-the-banking-and-insurance-sectors.

9.13 Regarding the role played by the PRA and the regulatory authorities in the event of disruption to national critical infrastructure, part of the Bank's operational resilience programme involves responding to operational shocks when they occur. This requires the financial sector and authorities to have well-rehearsed contingency plans and incident response processes, which are critical for minimising impact and continuing to deliver essential services to an acceptable level during operational disruption.

9.14 The UK financial authorities (HM Treasury, the Bank of England and the Financial Conduct Authority) have a single mechanism to coordinate a response to incidents that have affected, or have the potential to affect, the financial sector. It now includes the National Cyber Security Centre (NCSC) and, when appropriate, the National Crime Agency (NCA) for cyber incidents.

9.15 The Bank of England regularly exercises its response frameworks together with the sector to prove plans work and identify improvements. Some of these exercises have led to the development of industry-owned resilience playbooks, which set out coordinated approaches to dealing with a particular scenario.[27]

9.16 Regarding penetration (PEN) testing, one respondent noted that it would be difficult to expect firms to conduct their own PEN testing on material outsource providers. They suggested instead that firms have access to the results of any PEN testing conducted by or on behalf of the providers themselves.

9.17 In light of this response, the PRA has decided to amend paragraph 8.4 of the SS to clarify that access, audit and information rights in material outsourcing arrangements should include where relevant the results of security penetration testing by the outsourced service provider on its applications, data, and systems. In addition, the PRA has also clarified in Chapter 10 of the SS that for firms subject to the CBEST framework, the CBEST Implementation Guide notes that 'malicious Insider and Supply Chain Scenarios are a feature of the threat landscape for many firms. These scenarios should always be analysed and discussed during CBEST'. Where required, these firms 'should plan in advance the involvement of staff and third parties to increase the reality of assessment'. This expectation is in line with the CBEST Implementation Guide published in January 2021.[28]

27 February 2021: https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity.
28 January 2021: https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide.

10 Sub-outsourcing

10.1 The CP noted that sub-outsourcing can amplify certain risks in material outsourcing arrangements, for example relating to data security, and can limit firms' ability to manage them, particularly where large, complex chains of service providers are involved. The draft SS proposed a number of expectations to ensure that firms appropriately manage the risks of sub-outsourcing.

Scope and responsibilities

10.2 The PRA recognises that sub-outsourcing is a challenging regulatory area. Respondents noted that operational resilience provides a useful lens for assessing the risk of complex supply chains. Ten respondents asked the PRA to clarify that the expectations in this chapter apply only to material sub-outsourcing. Sixteen respondents also requested that the PRA provide greater clarity regarding the allocation of responsibilities between firms and third party services providers regarding the oversight and monitoring of fourth parties.

10.3 Having considered these responses, the PRA has:

- clarified that the detailed expectations on sub-outsourcing apply only to material sub-outsourcing. Firms should use the materiality criteria set out in Chapter 5 of the SS when determining if sub-outsourcing is material, including the potential impact on the firm's ability to deliver important business services within its impact tolerances;

- clarified that a firm is expected to ensure that its service provider appropriately manages any material sub-outsourcing. The PRA does not expect firms to directly monitor fourth or fifth parties. However, when entering into a material outsourcing agreement, firms should pay particular attention to the potential impact of large, complex sub-outsourcing chains on their operational resilience, including the potential effect on their ability to remain within impact tolerances during operational disruption. Firms should also consider whether extensive sub-outsourcing could compromise their ability to oversee and monitor an outsourcing arrangement; and

- noted that sometimes the same service provider may have both a direct contractual relationship with a firm and also be a sub-outsourced service provider to that firm via the supply chains of other service providers. In such situations, where appropriate, firms may leverage their direct contractual relationship with the service provider to assess its resilience in respect of all the services for which it relies on that provider, including those where they have a dependency on that service provider via the supply chain of other third parties.

Termination rights

10.4 Two respondents requested additional examples to illustrate when firms may choose to exercise termination rights in relation to sub-outsourcing. In light of these responses, some non-exhaustive examples have been incorporated into the SS.

Intragroup sub-outsourcing

10.5 Five respondents requested additional information on how sub-outsourcing arrangements could be applied proportionately in an intragroup context. Likewise, one respondent asked for further guidance on how proportionality could be applied when sub-outsourcing to a regulated firm.

10.6 Having considered these responses, the PRA has clarified in Chapter 3 of the SS that when a firm receives outsourcing services through an intragroup outsourcing arrangement, it is unlikely to have a direct contractual relationship with the external third party service provider, but may instead

receive services via an intragroup outsourcing arrangement. In this scenario, the firm can rely on assurance from the relevant group or parent entity providing the service as long as this assurance takes into account its own regulatory and resilience requirements. This may include escalating concerns about deteriorating service levels at the service provider to the group or parent entity, and relying on the group or parent entity to remediate them.

Direct requirements for service providers

10.7 One respondent suggested that the PRA consider requiring unregulated service providers to co-operate with the documentation of sub-outsourcing. They requested clarification on whether the PRA can impose contractual obligations directly on service providers regarding sub-outsourcing.

10.8 The PRA can only address its expectations to regulated firms. However, the PRA encourages service providers to facilitate firms' assessment of sub-outsourcing by, for instance, providing a list of, as a minimum, their material sub-outsourced providers.

10.9 Four respondents noted that it would be difficult to negotiate access, audit, and information rights for material sub-outsourcing arrangements.

10.10 Having considered these responses, the PRA notes that access, audit, and information rights for material sub-outsourcing arrangements are already expected under the EBA Outsourcing GL and in Article 274 of the Solvency II Delegated Regulation as it forms part of retained EU law. As noted in relation to wider feedback on the difficulty of securing the appropriate contractual provisions, the PRA recognises that negotiating with suppliers present challenges. An expectation has been added in paragraph 6.5 of the SS, which sets out that if an outsourced service provider in a material outsourcing arrangement is unable or unwilling to contractually facilitate a firm's compliance with its regulatory obligations and expectations, firms should make the PRA aware of this.

Miscellaneous

10.11 CP30/19 noted that to facilitate firms' assessment of the risks of sub-outsourcing, service providers could maintain up-to-date lists of the entities to which they sub-outsource services and functions. Two respondents commented on this. They requested that the PRA specify which sub-outsource providers would qualify for inclusion on the list. The PRA has not made any changes in response to this feedback as it considers that it is for firms to discuss with service providers the content of any list.

11 Business continuity and exit planning

11.1 The CP proposed to include an expectation that for each material outsourcing arrangement, firms should develop, document, maintain, and test a business continuity plan and exit strategy, which should cover and differentiate situations where a firm exits an outsourcing agreement due to a stressed or non-stressed exit.

Timing

11.2 Eight respondents requested clarity on when in the outsourcing lifecycle firms should develop and test their business continuity and exit plans. There was a range of views, but several respondents noted that while it was possible to begin developing plans in the pre-outsourcing phase, full testing was difficult until after the contract was signed.

11.3 Having considered these responses, the PRA has amended the SS to clarify that before a contractual agreement becomes effective, firms should evaluate what would be involved in delivering an effective stressed exit and use this to formulate their exit plan. Firms should seek to test the stressed exit plan as soon as practically possible. Where possible and relevant, testing should take place in a suitable, non-live environment. Once the arrangement has been implemented, firms should test their business continuity and exit plans using a risk-based approach. Where possible and relevant, this testing should align to, support, or even be a component of firms' scenario testing, as required under operational resilience policy.

Intragroup exit planning

11.4 Four respondents asked for further guidance in relation to intragroup exit planning. They noted that in the context of intragroup outsourcing, material deterioration in service is more likely to be resolved by internal escalation, rather than moving to a new supplier. Two respondents requested confirmation that firms that are subject to OCIR do not need to implement intragroup exit plans to fulfil the expectations in the SS.

11.5 Having considered these responses, the PRA has amended the SS to:

- clarify that for intragroup arrangements, firms' exit options might be considerably more limited than in other scenarios. This is particularly true for branches, which are unable to enter into standalone contractual arrangements with third parties. Nevertheless, the PRA expects these entities to take reasonable steps to try to identify options, however limited, to maintain the operational resilience of any important business services which they provide in the UK; and

- note in Chapter 3 that banks' compliance with requirements under OCIR may also mean that those banks meet the PRA's expectations on business continuity and exit planning.

Exit planning

11.6 Two respondents noted that the PRA's expectations, when applied to cloud outsourcing arrangements, could be interpreted as the PRA expressing a preference for the portability of the service.

11.7 In light of these responses, the PRA has clarified that it expects firms to assess the resilience requirements of the service and data that are being outsourced and, with a risk-based approach, decide on one or more available cloud resiliency options. The SS explicitly states that there is no hierarchy or one-size-fits-all combination of cloud resiliency options, and the optimal approach may well involve a combination of tools.

Operational resilience and business continuity and exit planning

11.8 One respondent requested clarity on whether the PRA expects testing to be carried out twice on a service where it forms part of an important business service, in addition to being a material outsourcing arrangement. In addition, the same respondent requested confirmation that the PRA expects that all outsourcing arrangements that support an important business service should be considered material. One respondent requested further information on the distinction between firm-level business continuity plans and those required for individual outsourcing arrangements.

11.9 Having considered this response, the PRA has not made any changes to the SS. The Operational Resilience Parts of the PRA Rulebook require firms to test their ability to remain within impact tolerances in severe but plausible disruption scenarios. Likewise, the SS expects that firms' testing of their business continuity and exit plans should include the ability to remain within impact tolerances. Firms may choose to conduct testing that fulfils both of these obligations at the same time. In addition, Chapter 5 of the SS notes that a key criterion for assessing materiality is whether an arrangement could materially impair the firm's operational resilience, particularly its ability to continue providing important business services. The PRA expects, therefore, that all outsourcing arrangements that support an important business service should be considered material.

Written agreement

11.10 Five respondents commented on whether it was appropriate or feasible for the PRA to expect that the written agreement should include the expectation that both parties implement and test business contingency plans, which take account of firms' impact tolerances for important business services. It was noted that a more practical approach would be to require that the firm and the service provider are required to implement and test their own business continuity and exit plans.

11.11 The PRA has considered these responses and amended paragraph 6.4 of the SS in line with the approach suggested.

Miscellaneous

11.12 One respondent noted that it was not necessary for a firm to have two distinct exit strategies covering stressed and non-stressed scenarios. The PRA confirms that one strategy that covers both stressed and non-stressed exits would be satisfactory.

11.13 One respondent requested further guidance on exit planning for their arrangements with financial market infrastructures (FMIs). The PRA has considered this response and chosen not to amend the SS. As noted in Chapter 2 of this PS, arrangements with FMIs are not considered outsourcing and firms are not expected to apply the detailed expectations on business continuity and exit planning.

11.14 One respondent noted that the draft SS referred to both 'exit strategies' and 'exit plans'. The PRA can confirm that these terms were used interchangeably. The SS has been revised to ensure the term 'exit plan' is used consistently.

11.15 One respondent argued that the resiliency offered by the cloud meant that a full exit plan should not be required. The PRA has considered this response and maintains that comprehensive exit planning is required for all material outsourcing arrangements regardless of whether they involve cloud technology.

11.16 One respondent requested that the PRA clarify whether firms should include commercial and unplanned exits from an outsourcing arrangement as a 'severe but plausible' scenario that could be tested in fulfilment of the operational resilience requirements. The PRA considers that commercial

exit due to a stressed scenario (eg failure or insolvency of the service provider) could be an appropriate 'severe but plausible' scenario. As noted in SS1/21 when setting scenarios, firms could consider previous incidents or near misses within the organisation, across the financial sector and in other sectors and jurisdictions. A testing plan should include realistic assumptions and evolve as the firm learns from previous testing. The nature and severity of scenarios that it is appropriate for firms to use may vary according to their size and complexity. As such, the PRA does not consider that it would be helpful to provide detailed guidance or examples.

11.17 Three respondents requested that the PRA clarify whether firms should consider 'all potentially viable forms of exit' and to consider 'all available tools' that could facilitate an exit. It was noted that such an expectation would be disproportionate. The SS has been revised to make the expectation more proportionate in light of these responses.

12 Systemic concentration risk

12.1 In the CP, the PRA noted that a single service provider, or a small number of service providers which are very difficult to substitute may, in some cases, dominate the provision of certain outsourced and third party services to large numbers of PRA-regulated firms. The failure of or a prolonged, significant disruption at a critical third party could have adverse consequences on financial stability. The CP invited responses on how the potential impact of all critical third parties on financial stability could be better assessed, monitored and managed both domestically and internationally in a way that helps advance financial stability and promote the operational resilience of firms, and signalled that the PRA may, in due course, further refine its approach and make future changes.

12.2 Seventeen respondents provided responses on this topic ranging from firms to trade associations and third party service providers. There was strong consensus among respondents that there are limits on what firms can do to mitigate or manage potentially systemic, market-wide concentration risk. Most respondents noted that systemic concentration risk could not be appropriately identified by individual firms working in isolation and urged caution against an over-reliance on firms' responsibility to assess, monitor, and manage it. Several respondents concluded that regulatory authorities, not individual financial institutions, were best positioned to assess systemic concentration risk.

12.3 A number of respondents highlighted the importance of effective data to identify concentration risk in critical, non-regulated service providers. Respondents urged regulators to help firms identify common critical third parties widely used across the industry and expressed support for the idea of a central register where firms provide their existing third party data in a consistently structured format.

12.4 Several respondents encouraged further consideration of how regulators can or may intend to take action for third parties that operate outside the regulatory perimeter. One respondent noted that the PRA and other international regulators should work together and engage with the largest technology vendors to discuss their operational resilience and what measures could be taken during a potentially systemic event. However, respondents cautioned that action by the regulators should not restrict the choice of outsourcing arrangements or providers available to firms, which would cause difficulties and could require undesirable sacrifices to security, efficiency, and innovation. Instead, regulators should focus on reducing the risks arising from concentration rather than reducing concentration itself. One respondent noted that lessons learnt from other areas of the industry where concentration exists and is accepted and managed, such as central clearing, could be applied to other outsourced service providers where firms are not yet critically dependent. One respondent suggested leveraging the implementation of important business services and impact tolerances (which include financial stability impacts for 'severe but plausible events' for the loss of important suppliers). Another respondent recommended adding a reference to site reliability engineering functions in PRA guidance.

12.5 In response to these comments, the importance of this topic and regulatory developments around the world, the PRA considers that further constructive dialogue, both internally and with industry and other stakeholders, on how to address the challenges stemming from systemic concentration risk may be beneficial. The PRA recognises the importance of developing pragmatic solutions to address the potential financial stability risks that may arise from systemic concentration without unduly restricting innovation.

12.6 As signposted in Chapter 1, the PRA is planning a follow-up consultation setting out detailed proposals for an online portal that all firms would need to populate with certain information on their outsourcing and third party arrangements or a subset thereof, such as those deemed material.

12.7 The PRA also intends to undertake further analysis on whether additional policy measures to manage the risks that critical third parties could pose to their objectives might be appropriate. Subject to the outcome of this analysis, the PRA may bring forward further proposals.

Appendix

1 **SS2/21 'Outsourcing and third party risk management', available at: www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss.**