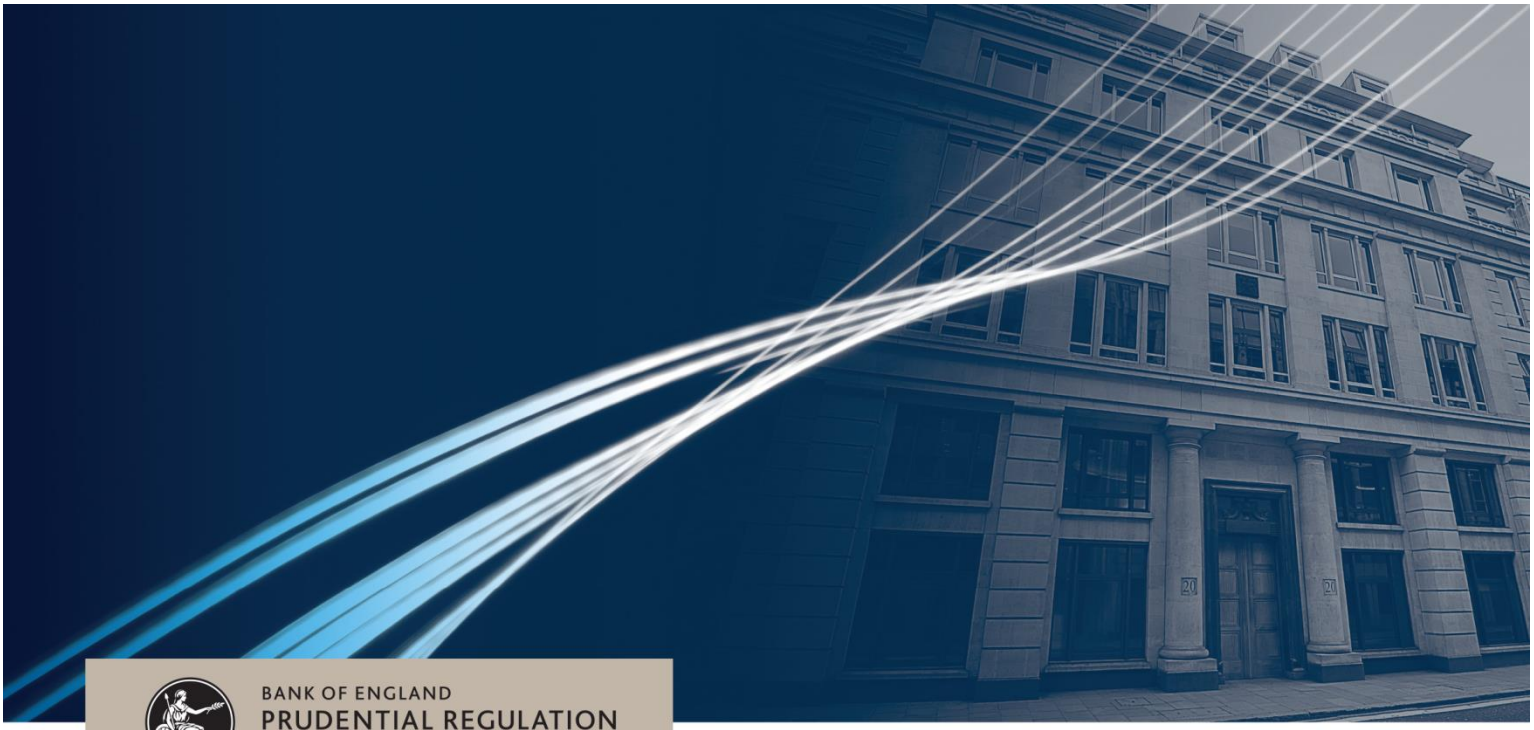

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Consultation Paper | CP30/19

# Outsourcing and third party risk management

December 2019

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Consultation Paper | CP30/19

# Outsourcing and third party risk management

December 2019

By responding to this consultation, you provide personal data to the Bank of England. This may include your name, contact details (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself.

The response will be assessed to inform our work as a regulator and central bank, both in the public interest and in the exercise of our official authority. We may use your details to contact you to clarify any aspects of your response.

The consultation paper will explain if responses will be shared with other organisations (for example, the Financial Conduct Authority). If this is the case, the other organisation will also review the responses and may also contact you to clarify aspects of your response. We will retain all responses for the period that is relevant to supporting ongoing regulatory policy developments and reviews. However, all personal data will be redacted from the responses within five years of receipt. To find out more about how we deal with your personal data, your rights or to get in touch please visit bankofengland.co.uk/legal/privacy.

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure to other parties in accordance with access to information regimes including under the Freedom of Information Act 2000 or data protection legislation, or as otherwise required by law or in discharge of the Bank's functions.

Please indicate if you regard all, or some of, the information you provide as confidential. If the Bank of England receives a request for disclosure of this information, we will take your indication(s) into account, but cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system on emails will not, of itself, be regarded as binding on the Bank of England.

Responses are requested by Friday 3 April 2020.

**Please address any comments or enquiries to:**
Orlando Fernández
Prudential Regulation Authority
20 Moorgate
London
EC2R 6DA

Email: CP30_19@bankofengland.co.uk

## Contents

# 1 Overview

1.1 In this consultation paper (CP), the Prudential Regulation Authority (PRA) sets out and invites comments on its proposals for modernising the regulatory framework on outsourcing and third-party risk management. These proposals are set out in the draft Supervisory Statement on 'Outsourcing and third party risk management' in the Appendix to this CP (draft SS) and pursue the following objectives:

- complement the policy proposals on operational resilience in CP29/19 'Operational resilience: impact tolerances for important business services', published simultaneously with this CP.[1]

- facilitate greater resilience and adoption of the cloud and other new technologies as set out in the Bank of England (the Bank)'s response to the 'Future of Finance' report.

- implement the European Banking Authority (EBA) 'Guidelines on Outsourcing Arrangements' (EBA Outsourcing Guidelines).[2] The draft SS clarifies how the PRA expects banks to approach the EBA Outsourcing Guidelines in the context of its requirements and expectations. In addition certain chapters in the draft SS elaborate on the expectations in the EBA Outsourcing Guidelines. For instance, chapters 7 (Data Security) and 10 (Business Continuity and exit plans).[3]

- Take into account the:

    - draft European Insurance and Occupational Pensions Authority (EIOPA) 'Guidelines on Outsourcing to Cloud Service Providers (EIOPA Cloud Guidelines')[4]; and

    - EBA Guidelines on ICT and security risk management (EBA ICT Guidelines);[5]

1.2 This CP is relevant to all UK:

- banks, building societies and PRA-designated investment firms (hereafter 'banks');

- insurance and reinsurance firms and groups in scope of Solvency II, including the Society of Lloyd's and managing agents (hereafter 'insurers'); and

- branches of overseas banks and insurers (hereafter 'third country branches')'.

- Banks, insurers and third country branches are collectively referred to as 'firms' in this CP and the draft SS.

1.3 Some of the proposals in this CP are relevant to credit unions and non-directive firms (NDFs) namely those in: paragraph 2.3 of this CP; the PRA rules, statutory powers and requirements referenced in tables 2, 5 and 6; and paragraphs 5.11-5.12. In line with the principle of

1 https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.
2 https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.
3 The terms contingency plan and continuity plan stem from European legislation. They are used interchangeably in this CP.
4 https://eiopa.europa.eu/Publications/Consultations/2019-07-01%20ConsultationDraftGuidelinesOutsourcingCloudServiceProviders.pdf.
5 At the time of publication of this draft SS for consultation, the draft EIOPA Cloud Guidelines had not been finalised. Subject to the final form of these Guidelines, our final policy and the final version of the SS in Annex 1 may be updated accordingly.

proportionality, the PRA proposes not to apply the remaining sections of the draft SS to credit unions and NDFs.

1.4 The proposals for insurers take into account the requirements and expectations in:

- Solvency II;
- Commission Delegated Regulation 2015/35 supplementing Solvency II (Solvency II Commission Delegated Regulation);
- the EIOPA Guidelines on the System of Governance (EIOPA Governance Guidelines);[6] and
- the draft EIOPA Cloud Guidelines.

1.5 However, unlike the proposals in the draft EIOPA Cloud Guidelines, the PRA's proposals would cover all outsourcing and, where indicated, third-party arrangements entered into by insurers – not just those relating to Cloud. The PRA considers that a clear and consistent set of expectations for banks and insurers relating to all forms of outsourcing and, where indicated, third-party arrangements will advance its objectives, including on policyholder protection.

## Further Policy Development

1.6 The proposals in this CP have been designed in the context of the current UK and EU regulatory framework. In the event that the UK leaves the EU with no implementation period in place, the PRA has assessed that the proposals would not need to be amended under the EU (Withdrawal) Act 2018 (EUWA). Please see PS5/19 'The Bank of England's amendments to financial services legislation under the European Union (Withdrawal) Act 2018'[7] for further details.

- The draft SS attached to this CP should be read in conjunction with SS1/19 'Non-binding PRA materials: The PRA's approach after the UK's withdrawal from the EU'.[8]
- As these proposals relate to EU Guidelines, they should be read in conjunction with the joint Bank and PRA Statement of Policy (SoP) 'Interpretation of EU Guidelines and Recommendations: Bank of England and PRA approach after the UK's withdrawal from the EU'.[9]

1.7 The PRA will keep monitoring developments in industry practice and the international regulatory landscape to assess whether changes to the proposals in this CP and the draft SS are required and whether they should be subject to further consultation. In particular, the following areas could trigger a requirement for further consultation:

- The proposals in this CP and the draft SS take into account the draft EIOPA Guidelines and the EBA ICT Guidelines. However, these Guidelines have not been finalised at the time of publication of this CP and could undergo changes due to consultation feedback. The PRA will consider its approach to these Guidelines once they are finalised and published.
- Discussions and potential future regulatory developments relating to systemic concentration risk, systemically significant third parties and their potential implications on financial stability are

6 https://eiopa.europa.eu/publications/eiopa-guidelines/guidelines-on-system-of-governance.
7 April 2019: https://www.bankofengland.co.uk/paper/2019/the-boes-amendments-to-financial-services-legislation-under-the-eu-withdrawal-act-2018.
8 April 2019: https://www.bankofengland.co.uk/prudential-regulation/publication/2019/non-binding-pra-materials-the-pras-approach-after-the-uks-withdrawal-from-the-eu-ss.
9 April 2019: https://www.bankofengland.co.uk/paper/2019/interpretation-of-eu-guidelines-and-recommendations-boe-and-pra-approach-sop.

taking place and are expected to continue in international fora. Over time this could result in changes to the regulatory framework.

- In this CP, the PRA is consulting on the idea of developing an online portal for the register. If it goes ahead, the development of this portal would take place on a longer timeframe to the other proposals in this CP and would require additional consultation on its specific form and characteristics.

## Background

1.8 Firms' reliance on third parties, in particular through outsourcing arrangements, is well-established and has been subject to regulatory requirements and expectations for over a decade. However, in recent years, firms' interactions with third parties have evolved significantly. In particular, firms are increasingly relying on technology provided by third parties, such as the Cloud to gain entry to new markets, lower operating costs, fuel innovation and adapt to the digital economy. Cloud outsourcing has become a particular area of focus as the Cloud provides the underlying infrastructure supporting many technology solutions used by firms.

1.9 These changes in firms' reliance on outsourcing and third parties bring potential benefits and opportunities, including, in the case of Cloud, potentially enhanced resilience compared to firms' on-premise data centres (provided that firms oversee the provision of Cloud services effectively and take appropriate steps to protect their applications and data).

1.10 However, firms' evolving practices also create risks. For instance, ensuring that confidential, important or sensitive data outsourced to or shared with third parties is secure and accessible to firms and regulators, including during or following an operational disruption is both challenging and essential.

1.11 Moreover, the technical complexity of some technologies provided by third parties coupled with the fact that they are constantly evolving can make it difficult for firms' boards and senior management to understand and manage relevant risks. These difficulties can be amplified when service providers outsource parts of the services they have contracted to provide to firms to other service providers. This is known as 'sub-outsourcing' and it increasingly involves complex, long chains of service providers.

1.12 In addition, the provision of certain outsourced and third party services, such as the Cloud, which can be heavily dominated by a small group of service providers, may limit firms' ability to exit outsourcing arrangements without incurring significant costs, disruption, resources and time ('vendor lock-in').

1.13 Moreover, if a large number of firms become dependent on a small number of dominant outsourced or third party service providers who are very difficult or impossible to substitute, this could, over time, give rise to systemic concentration risks. A major disruption, outage or failure at one of these service providers could create a single-point-of-failure with potential adverse consequences for financial stability.

1.14 Against this background, supervisory authorities around the world are updating their rules, expectations, guidance and supervisory practices on outsourcing and third party risk management. In the UK, this process is well-aligned to the:

- development of a regulatory framework on operational resilience, as proposed in CP29/19; and

- publication of the 'Future of Finance' report[10] and the Bank's response to it, which examine 'the future of the UK financial system, and what it might mean for the Bank's agenda, toolkit and capabilities over the coming decade' with an emphasis on how the Bank can 'enable innovation, empower competition and build resilience'.

1.15 The proposals in this CP seek to modernise the PRA's expectations relating to outsourcing and third party risk management through the draft SS in the Appendix, which sets how the PRA expects firms to comply with the wide range of existing requirements on outsourcing and third party risk management, throughout the lifecycle of an arrangement.

1.16 The proposals in this CP and the draft SS apply to all forms of outsourcing and, where indicated, third party arrangements. However, they include examples, references and sections addressing specific issues of particular relevance to Cloud outsourcing, such as data security, business continuity and exit planning (see chapters 7 and 10 of the draft SS). By addressing these issues, the draft SS seeks to provide 'conditions that can help give firms assurance' to enable firms to deploy the Cloud 'in a safe and resilient manner' in line with the Bank's response to the 'Future of Finance' report. The PRA would particularly welcome views on areas where additional regulatory certainty on the use of Cloud would be beneficial.

## Implementation

1.17 The PRA proposes to publish its final policy on the proposals in this CP in the second half of 2020 (in line with the final policy on Operational Resilience), with implementation of most the proposals shortly after.

1.18 Certain proposals in this CP, which derive from the EBA Outsourcing Guidelines or (if adopted in the current form) the draft EIOPA Cloud Guidelines would be subject to longer implementation periods. In particular, those relating to:

- the register of outsourcing arrangements ('Outsourcing Register'); and
- the revision by:
    - banks of outsourcing arrangements entered into before 30 September 2019; and
    - insurers of cloud Outsourcing arrangements entered into before 1 July 2020 ('Legacy Outsourcing Arrangements') to bring them into compliance with the EBA Outsourcing Guidelines and EIOPA Cloud Guidelines respectively.

### Outsourcing Register

1.19 The EBA Outsourcing Guidelines provide that banks should gradually build an Outsourcing Register which should be complete by 31 December 2021. Banks are expected to include in their Outsourcing Register:

- new outsourcing arrangements entered into from 30 September 2019 onwards; and

10 https://www.bankofengland.co.uk/report/2019/future-of-finance.

- Legacy Outsourcing Arrangements as they become due for review or renewal, with a view to having a complete Outsourcing Register by 31 December 2021.

1.20 The 'EBA Recommendations on Outsourcing to Cloud Service Providers' currently provide for banks to maintain a register of all their Cloud outsourcing arrangements ('Cloud Register').[11] This expectation will continue for banks until the deadline to have a complete Outsourcing Register becomes effective and the Outsourcing Register subsumes the Cloud Register on 31 December 2021.

1.21 Subject to the outcome of the consultation on the draft EIOPA Cloud Guidelines, insurers may also be expected to maintain a Cloud Register from 1 December 2020.

1.22 As set out in Chapter 4 of the draft SS, the PRA proposes that we will expect all firms to maintain their own Outsourcing Register. As noted in paragraph 1.7, the PRA is also considering the idea of an online portal where firms would submit the information in the Outsourcing Register. If it goes ahead, this would take place on a longer timeline than the proposals in this CP and the draft SS and be subject to further consultation. The PRA would particularly welcome views on the Outsourcing Register and the idea of an online portal, including the potential practicalities and timeline for development and implementation.

### Legacy Outsourcing Arrangements

1.23 The EBA Outsourcing Guidelines expects banks to:

- review Legacy Outsourcing Arrangements entered into before 30 September 2019 and amend them to ensure they comply with the EBA Outsourcing Guidelines; and

- inform the PRA of any Legacy Outsourcing Arrangements of critical or important operational functions (referred to as material outsourcing arrangements in this CP and the draft SS) that have not been reviewed by 31 December 2021, including the measures planned to complete the review or the possible exit strategy.

1.24 The PRA is not proposing changes to the timeline for reviewing Legacy Outsourcing Arrangements in the EBA Outsourcing Guidelines. The PRA may agree an extended timeline with firms for completing the review of Legacy Outsourcing Arrangements on a case-by-case basis if appropriate.

1.25 The draft EIOPA Cloud Guidelines propose to expect insurers to:

- review and amend existing Cloud outsourcing arrangements entered into before 1 July 2020 (Legacy Cloud Outsourcing Arrangements), with a view to ensuring that these are compliant with the proposed Guidelines by 1 July 2022; and

- inform the PRA of any material Legacy Cloud Outsourcing Arrangements whose review has not been finalised by 1 July 2022, including the measures planned to complete the review or the possible exit strategy.

11 https://eba.europa.eu/documents/10180/2170121/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf.

## Treasury Select Committee (TSC) report on 'IT failures in the Financial Services Sector'[12]

1.26 On Monday 28 October 2019, the TSC published a report following its inquiry into IT failures in financial services, which included recommendations to improve operational resilience in the financial sector. The supervisory authorities have reviewed the TSC's report and note that the proposals are consistent with TSC's recommendations where relevant. The supervisory authorities will provide a full response to all the TSC's recommendations in due course.

1.27 A key objective of the proposals in this CP and the draft SS is to clarify, strengthen and update the PRA's expectations on how firms should manage outsourcing and third party risks. For instance by:

1.28 promoting consistent, structured and thorough vendor due diligence and pre-contractual assessments of the materiality and risks of outsourcing arrangements;

1.29 specifying minimum contractual safeguards that material outsourcing arrangements should meet;

1.30 setting out the PRA's expectations on how firms should protect data they outsource; and

1.31 developing, documenting and testing robust business continuity plans and exit strategies to improve their ability to withstand and recover from potential failures and outages in material third party service providers in a manner that promotes their operational resilience.

1.32 This CP and draft SS also include chapters dedicated to exploring some of the 'ways to mitigate concentration risk' referred to in the TSC Report. For instance,

1.33 'utilising the EBA process of leveraging pooled audit arrangements for cloud service providers' (Chapter 7 of the SS); and

1.34 'potentially building applications able to substitute a critical supplier with another' (Chapter 10 of the SS)

1.35 The proposals on the Outsourcing Register will also enable the PRA and the FCA to develop a better understanding of the sector's reliance on different parties.

1.36 The majority of the proposals in this CP focus on the PRA's expectation of how firms should manage outsourcing and third party risks, however paras.2.48-2.53 of this CP focus on the topic of systemic concentration risks and outline some of the ongoing work undertaken in this area, including by the FPC. The CP also invites industry feedback on how these systemic concentration risks 'could be better assessed, monitored and managed both domestically and internationally'.

## Responses and next steps

1.37 This consultation closes on Friday 3 April 2020. The PRA invites feedback on the proposals set out in this consultation. Please address any comments or enquiries to CP30_19@bankofengland.co.uk.

12 https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/news-parliament-2017/it-failures-financials-services-sector-report-published-19-20/

# 2 Proposals

2.1 The proposals in this CP would be implemented via the draft SS, which comprises the following chapters:

- Introduction (Chapter 1);
- Definitions and scope (Chapter 2);
- Proportionality (chapter 3);
- Governance and record-keeping (chapter 4);
- Pre-outsourcing phase (chapter 5);
- Outsourcing agreements (chapter 6);
- Data security (chapter 7);
- Access, audit and information rights (chapter 8);
- Sub-outsourcing (chapter 9); and
- Business continuity and exit plans (chapter 10).

2.2 Table 1 in the draft SS sets out some of the main sources of law applicable to outsourcing by firms. The proposals in this CP and the draft SS should be read in conjunction with these and other applicable legal requirements and expectations, and interpreted and applied consistently with them.

2.3 As noted in Chapter 1 of this CP, the PRA does not propose to apply most of the proposals in this CP to credit unions and NDFs. However, it proposes a general expectation that credit unions and NDFs manage the risks in their outsourcing and third party arrangements prudently. The PRA will take into account the extent to which they have done so when assessing their compliance with the requirements in Table 2 in the draft SS.

## Definitions and scope

2.4 The PRA Rulebook defines outsourcing as 'an arrangement of any form between a firm and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be undertaken by the firm itself'.

2.5 The definition of 'outsourcing' in the PRA Rulebook derives from Article 2(3) of Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (MODR)[13] and Article 13(28) of Solvency II.[14] They do not apply to arrangements between firms and third parties falling outside this definition.

13 http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/78111/03-12-2019
14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0565.

2.6 As noted in the EBA Outsourcing Guidelines and draft EIOPA Cloud Guidelines, it is for firms to assess whether an arrangement with a third party/Cloud service provider falls within the definition of 'outsourcing'. However, consistent with the draft EIOPA Cloud Guidelines, the PRA proposes firms to assume that activities, functions and services performed or provided by third parties in a 'prudential context' as defined in the PRA Rulebook,[15] fall within the definition of 'outsourcing' and apply the remaining expectations in the draft SS to them (which will vary depending on their 'materiality' as examined in Chapter 5 of the draft SS).

2.7 Moreover, some arrangements between firms and third parties (third party arrangements) which may fall outside the definition of 'outsourcing' in the EBA Outsourcing Guidelines may also be relevant to: the financial stability of the UK; the PRA's statutory objectives; the operational resilience of firms; and/or the performance of regulated activities or the Bank's resolution objectives. For instance, the sharing of data with third parties, including through application programming interfaces (APIs);[16] the purchase of third party hardware or software eg 'off the shelf' artificial intelligence/machine learning (AI/ML) models; and the use of aggregators by insurance firms.

2.8 Third party arrangements falling outside the definition of 'outsourcing' may not be subject to specific requirements on outsourcing. They are however within the scope of the PRA's Fundamental Rules and general requirements and expectations, particularly on governance, risk management and systems and controls. The draft SS therefore reminds firms of their obligation to comply with the following PRA rules in relation to all their arrangements with third parties, irrespective of whether they fall under the definition of outsourcing:

- Fundamental Rules 2, 3, 5 and 6 in the Fundamental Rules Part of the PRA Rulebook;
- the Conduct Rules and Insurance - Conduct Standards and Senior Manager Conduct Rules/Standards Parts;
- the General Organisational Requirements (banks) and Chapter 2 of the Conditions Governing Business (insurers) Parts of the PRA Rulebook, which include requirements on business continuity, contingency planning and data protection; and
- the Risk Control Part of the PRA Rulebook (banks) and Conditions Governing Business 3 (insurers).

2.9 In addition, the PRA is consulting separately on new rules on operational resilience in CP29/19, which has been published simultaneously with this CP. In that CP (and subject to the outcome of both consultations), the PRA is proposing to apply the requirements in the Operational Resilience Parts of the PRA Rulebook and the Operational Resilience Chapter in the Group Supervision Part of the Rulebook (and accompanying expectations in the SS and Statement of Policy included in CP29/19) to all arrangements between firms and third parties, including but not limited to:

- draft Rule 4.1, which would require firms to identify and document 'the necessary people, processes, technology, facilities and information required to deliver each of its important business services'; and
- draft Rule 2.5, which would require firms to 'remain within its impact tolerance for each important business service in the event of a severe but plausible disruption to its operations'.

---

15 http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/53225/09-08-2019.
16 See Basel Committee on Banking Supervision, Report on open banking and application programming interfaces, November 2019 https://www.bis.org/bcbs/publ/d486.pdf.

## Proportionality

2.10 The PRA proposes that firms would comply with the proposed expectations in this CP in a manner appropriate to their size, internal organisation, risk profile, and the nature, scope and complexity of their activities. This is referred to as 'proportionality'.

2.11 Chapter 3 of the draft SS explains how proportionality would apply to the expectations in it. In particular in relation to intra-group outsourcing and 'non-significant' firms defined as those in categories 3 and below for the purposes of the draft SS (and consistently with other PRA Policy Statements (PSs) and SSs).[17]

2.12 'Proportionality' is separate but complementary to the concept of 'materiality' examined in Chapter 5 of the draft SS. Proportionality focuses on the characteristics of a firm, including its systemic significance; 'materiality' assesses the potential impact of a given outsourcing arrangement on a firm's safety and soundness, including its operational resilience.

2.13 Intra-group outsourcing is not inherently less risky than outsourcing to service providers outside a firm's group and is not treated differently under existing requirements. However, in line with Articles 31(4) of MODR[18] and 274(2) of the Solvency II Commission Delegated Regulation,[19] firms may take into account the level of 'control and influence' they have over any companies in their group they outsource services to when complying with the relevant requirements and expectations on outsourcing in MODR and the Solvency II Commission Delegated Regulation.

2.14 The PRA proposes to provide additional guidance on the notion of 'control and influence' in the draft SS and provide examples of areas where it may be possible for firms that enter into intra-group outsourcing arrangements to adopt a more proportionate approach to meeting the expectations included therein. One such example may be the extent of their due diligence.

2.15 The PRA also proposes to highlight in the draft SS certain expectations which 'non-significant' firms may be able to meet proportionately. For example, regarding the exercise of access and audit rights in Chapter 7 of the draft SS.

## Governance

2.16 The PRA proposes to set out expectations in the draft SS regarding:

- board engagement on outsourcing;
- the requirement on firms to meet the Threshold Conditions at all times and avoid becoming 'empty shells';[20]
- the application of the Senior Managers and Certification Regime (SM&CR) to outsourcing. In particular, the Prescribed Responsibility in Allocation of Responsibilities 4.1(21) (banks) and Insurance-Allocation of Responsibilities 3.1(A3)(12) (insurers); and

17 See PS7/13 - Strengthening capital standards: implementing CRD IV, feedback and final rules: https://www.bankofengland.co.uk/prudential-regulation/publication/2013/strengthening-capital-standards-implementing-crd-4, and SS10/16 Solvency II: Remuneration requirements https://www.bankofengland.co.uk/prudential-regulation/publication/2016/solvency-2-remuneration-requirements-ss.
18 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0565&from=EN.
19 https://eur-lex.europa.eu/mwg-internal/de5fs23hu73ds/progress?id=cGh0qFQs5fJ-OpWEOVpBgI2OFL5jsUqT-T6uD54nvUs,&dl.
20 See paragraph 39 of EBA Outsourcing Guidelines https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements,

- the contents of the outsourcing policy that firms are:
    - expected to maintain under the EBA Outsourcing Guidelines ad EBA Governance Guidelines (banks); and
    - required to maintain under Conditions Governing Business 2.4(1) (insurers).

## Record-keeping

2.17 Paragraphs 1.19-1.22 in this CP summarise the PRA's proposals regarding the Outsourcing Register. As noted in paragraph 1.7, these may be subject to further consultation.

2.18 In the meantime, the PRA proposes to include guidance in Appendix 1 of the draft SS on how firms should fill in certain fields which the EBA and EIOPA include in the Outsourcing Register/ [draft] Cloud Register. This guidance seeks to ensure that firms fill in the qualitative information in these Registers (eg the names of service providers) consistently as failure to do so can render comparative analysis difficult for the PRA. The PRA would particularly welcome feedback in this area to help inform the consistency and design of the Outsourcing Register.

2.19 There are a number of existing and proposed record-keeping requirements and expectations applicable to at least some firms that may partly overlap with the Outsourcing Register, for instance, under structural reform and the end-to-end mapping proposals of important business services in CP29/19. The PRA would welcome suggestions as to how firms' record keeping can satisfy the PRA's various record keeping requirements most efficiently.

2.20 The PRA would also be interested in views on the pros and cons of broadening the Outsourcing Register to include at least those third party arrangements outlined in paragraphs 2.5 and 2.6 of the draft SS.

## Pre-outsourcing phase: materiality assessment, due diligence and risk assessment

### Materiality assessment

2.21 The PRA Rulebook defines 'material outsourcing' as the outsourcing of 'services of such importance that weakness, or failure, of the services would cast serious doubt upon the firm's continuing satisfaction of the threshold conditions or compliance with the Fundamental Rules'.

2.22 Materiality includes the concept of a 'critical or important operational function' in applicable EU law. The most detailed requirements in Article 31 of MODR and Article 274(5) of the Solvency II Commission Delegated Regulation apply to the outsourcing of critical or important operational functions.

2.23 Although firms are responsible for assessing the materiality of outsourcing arrangements, there can be inconsistencies in their assessment criteria and conclusions.

2.24 There have also been instances where firms have notified the PRA of 'material outsourcing' arrangements too late for the PRA to meaningfully assess and discuss the arrangement and consider if additional steps were appropriate. The PRA therefore proposes to:

- introduce common criteria in the draft SS to improve the consistency of firms' materiality assessments. Some criteria, if met, would result in an expectation that the outsourcing arrangement should be automatically deemed material; and

- clarify that, in order the comply with Notifications 2.3(1)(e) and Fundamental Rule 7, the PRA expects firms to notify it of material outsourcing arrangements sufficiently in advance of entering into them to allow appropriate supervisory scrutiny.

### Due diligence and risk assessment

2.25 In line with the EBA Outsourcing Guidelines, the PRA proposes to include expectations in the draft SS on:

- firms' due diligence of prospective service providers; and

- the importance of assessing the risks of all outsourcing arrangements irrespective of their materiality. Firms' risk assessments should consider financial and operational risks and also take into account any risks which the outsourcing arrangement may mitigate or help the firm manage more effectively. The assessment should also consider concentration risks at the level of the firm or group eg extensive reliance on one service provider. The PRA would welcome views on whether and how firms currently assess concentration risks at the firm and group level, including any criteria used.

### Outsourcing agreements

2.26 Article 31(3) of MODR (banks) and 274(3)(c) of the Solvency II Commission Delegated Regulation require all outsourcing arrangements, irrespective of materiality and including intra-group arrangements, to be set out in a written agreement.

2.27 In line with the EBA Outsourcing Guidelines and draft EIOPA Cloud Guidelines, the PRA proposes to set out in the draft SS the areas that it expects, as a minimum, contracts for 'material outsourcing' arrangements to address. Four of these areas are subsequently examined in detail in chapters 7-10 of the draft SS, namely:

- data security (Chapter 7);

- access, audit and information rights (Chapter 8);

- sub-outsourcing (Chapter 9); and

- business continuity and exit plans (Chapter 10).

### Data security

2.28 The PRA proposes to include expectations in the draft SS on how firms should ensure that data in material outsourcing arrangements is adequately protected. These expectations build on General Organisational Requirements 2.4 (banks) and Article 274(e) of the Solvency II Commission Delegated Regulation (insurers) and note that firms should:

- define, document and understand their and their service providers' respective responsibilities in respect of data security (referred to as the 'shared responsibility model');

- identify and classify data based on its confidentiality and sensitivity and agree an appropriate level of confidentiality, availability and integrity;

- implement appropriate measures to protect outsourced data and include them in their outsourcing policies and outsourcing agreements. These measures should consider at a minimum:

    - The location of data, which should balance on a risk-based approach the potential:

        (i) resilience benefits of data being stored in multiple locations; and

        (ii) legal and practical challenges that firms and the PRA may experience if they need to access data located in certain jurisdictions.

    - Robust controls for data-in-transit, data-in-memory and data-at-rest. These controls should comprise both preventative and detective measures, which may include but not necessarily be limited to encryption and key management, identity and access management and incident detection and response.

### Access, audit and information rights

2.29 A key challenge in the negotiation of outsourcing agreements is ensuring that firms and regulators have appropriate rights to access, audit and request information from service providers.

2.30 The PRA has a range of statutory information-gathering and investigatory powers, some of which can apply directly to service providers in outsourcing arrangements (see Chapter 8 of the draft SS). In addition, Article 31(2)(i) of MODR, Article 274(4)(h)-(j) of the Solvency II Commission Delegated Regulation, chapters 2.2 and 3.3 of the Information Gathering Part of the PRA Rulebook (banks), and Conditions Governing Business 7.4 (insurers) set out requirements on access, audit and information rights.

2.31 The information-gathering and investigatory powers and PRA rules in paragraph 2.30 apply to all PRA-regulated firms including credit unions and NDFs. The PRA therefore reminds all firms subject to these provisions and requirements of the need to comply with them.

2.32 To ensure compliance with these and other applicable requirements, including those in the EBA Outsourcing Guidelines and draft EIOPA Cloud Guidelines, the PRA proposes to include an expectation in the draft SS that firms should take reasonable steps to ensure that written agreements for material outsourcing arrangements provide them, the PRA and (if applicable) the Bank as a resolution authority unrestricted access, audit and information rights to:

- enable firms to comply with their legal and regulatory obligations; and

- manage risks relating to the arrangement.

2.33 The PRA's proposals on effective access, audit and information rights should cover (as appropriate) premises, data, devices, information, systems and networks used for providing the service or monitoring its performance.

2.34 The PRA acknowledges the importance of access, audit and information rights being exercised in an outcomes-focused manner. To facilitate the effective exercise of these rights, the draft SS recognises various methods, which, subject to certain conditions, may enable firms to meet the expectations in the SS. For instance:

- certificates and reports facilitated by outsourced service providers (known as 'third party certification') if appropriately reviewed by the firm; or

- audits organised by groups of firms sharing one or more service providers (or facilitated by the service providers) and performed by representatives of the participating firms or specialists appointed on their behalf ('pooled audits').

### Sub-outsourcing

2.35 Sub-outsourcing can amplify certain risks in material outsourcing arrangements, eg on data security, and limit firms' ability to manage them; particularly where large, complex chains of service providers are involved.

2.36 The PRA therefore proposes that for material outsourcing arrangements which involve or may involve sub-outsourcing, firms:

- assess the risks of sub-outsourcing. Service providers can facilitate this by maintaining up-to-date lists of the entities they sub-contract functions and services to.

- pay particular attention to the potential impact of large, complex chains of sub-outsourced service providers on their operational resilience (in particular, the end-to-end provision of important business services).

- specify in written agreements for material outsourcing whether sub-outsourcing is allowed and, if so, subject to what conditions. They should also require service providers to:

    - notify firms ahead of planned material changes to sub-outsourcing in a timely manner;

    - obtain prior specific or general written authorisation where appropriate; and

    - give firms the right to approve or object to material sub-outsourcing arrangements and/or terminate the agreement in certain circumstances.

### Business Continuity and exit plans

2.37 Article 31(2)(l) Of MODR and Article 274 (4)(d) and (5)(d) of the Solvency II Commission Delegated Regulation as well as the EBA Outsourcing Guidelines, EBA Governance Guidelines and EBA IT Guidelines include requirements and expectations on business continuity planning, and for material outsourcing arrangements, exit plans.

2.38 The PRA proposes to include an expectation in the draft SS 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:

- disruption, an outage or the failure, ie insolvency or liquidation of the service provider ('stressed exit'); and

- commercial, performance or strategic reasons in a planned and managed way ('non-stressed exit').

2.39 Although the PRA proposes business continuity and exit plans would cover all material outsourcing arrangements, where relevant they should aim to enable firms to continue delivering important business services for which they rely wholly or in part on third parties, in line with their impact tolerances, following a disruption or stressed exit. The draft SS therefore focuses mainly on stressed exits rather than non-stressed exits.

### Business Continuity Plans

2.40 The PRA proposes that firms should implement and require service providers in material outsourcing arrangements to implement appropriate business continuity plans to anticipate, withstand, respond to and recover from severe but plausible disruption.

2.41 This expectation builds on existing PRA requirements on business continuity, eg General Organisational Requirements 2.3 and (subject to consultation) the proposed requirements and expectations on operational resilience.

2.42 In the specific case of material Cloud outsourcing arrangements, the PRA will expect firms to assess the resilience requirements of the outsourced service and data and determine which of the available Cloud resiliency options is most appropriate. These may include multiple availability zones, regions or service providers.

2.43 In line with the Bank's response to the 'Future of Finance' report's recommendations on enhancing data recovery, the PRA proposes that firms should consider the implications of deliberately destructive cyber-attacks when establishing or reviewing data recovery capabilities.

2.44 In the event of a disruption or emergency (including at an outsourced or third party service provider), firms should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the Bank, PRA and Financial Conduct Authority and, if relevant, the service providers themselves are informed in a timely and appropriate manner.

### Stressed exits

2.45 A key objective of stressed exit plans is to provide a risk mitigation of last resort in the event of disruption that cannot be managed through other business continuity measures. For instance, the cessation of business of a material outsourced service provider due to insolvency, liquidation or other reason.

2.46 The PRA does not have a preferred form of exit in stressed scenarios. Its focus is on ensuring that, if warranted, firms exit their outsourcing arrangements in a manner consistent with the PRA's statutory objectives, including as regards operational resilience, rather than the exit method itself. The draft SS therefore recognises a range of methods and proposes that firms should update their exit strategies periodically to take account of developments that may change the feasibility of an exit in stressed and non-stressed scenarios. For example, new technology tools which may facilitate the switching and portability of data and applications.

### Governance of business continuity plans and exit plans

2.47 The PRA also proposes to include expectations on the governance of business continuity and exit plans. For instance, the importance of firms:

- starting to develop these plans during the pre-outsourcing phase; and
- assigning clear roles and responsibilities and (where possible) convening multi-disciplinary teams to develop and execute these plans.

## Systemic concentration risks

2.48 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 (hereafter 'systemic third parties'). The failure of or a prolonged, significant disruption at a systemic third party could have adverse consequences on financial stability.

2.49 A small number of third parties have traditionally dominated the provision of certain functions, products of services to firms, such as cash machines or IT mainframes. However, the issue of systemic third parties is becoming an increasing area of focus for macro-prudential and micro-prudential regulatory authorities in the UK and internationally. This is because of a general increase in firms' reliance on third party service providers, as well as the emergence of new forms of outsourcing, such as Cloud. Systemic concentration creates the risk that disruption at one provider interferes with the provision of vital services by several firms. It was the possibility that third parties could act as a vector for a significant cyber-incidents that prompted the G-7 to devise their 'Fundamental Elements for Third Party Cyber Risk Management' in October 2018.[21]

2.50 There has also been much interest in the finance sector's planned uptake of Cloud services. In November 2018, the Financial Policy Committee (FPC) noted that 'if configured correctly, cloud services can significantly improve the operational resilience of individual financial firms, because the scale and expertise of Cloud service providers allows them to build resilience in a way that exceeds the capability of individual firms'. The FPC agreed to commence close monitoring of risks from the provision of Cloud services to the financial sector as part of its annual Risks Beyond Banking (RBB) review. In June 2019 the Bank's response to the 'Future of Finance' report also included commitments to:

- 'continue to work with firms to manage the risks associated with cloud outsourcing, including concentration risk and lack of substitutability; and to understand any tipping points for systemic risks from wider adoption'; and
- 'work with international standard-setting bodies, such as the Basel Committee on Banking Supervision (BCBS) and International Association of Insurance Supervisors (IAIS), to develop and adopt international standards [on Cloud]'.

2.51 The EBA Outsourcing Guidelines likewise note that 'competent authorities need to identify the concentrations of outsourcing arrangements at service providers' and note that 'if service providers, eg in the area of IT or fintech, fail or are no longer able to provide their services, including in the case of severe business disruption caused by external events, this may cause systemic risks to the financial market'. The data in firms' Outsourcing Register, if produced in and submitted in a clear and

---

21 G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector: https://www.fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf.

comparable format, could provide a valuable tool for the identification, monitoring and mapping of systemic third parties.

2.52 The primary purpose of the proposals in this CP and the draft SS is to strengthen and modernise the micro-prudential framework on all forms of outsourcing and third party risk management. In other words, to improve the ability of firms to manage relevant risks and facilitate oversight of outsourced and third party service providers by firms and the PRA.

2.53 However, discussions and potential future regulatory developments relating to the issue of systemic third parties and their potential implications on financial stability are taking place and set to continue in international fora. As noted in paragraph 1.7, as a result the PRA may, in due course, further refine its approach and make future changes. The PRA would therefore welcome feedback 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.

# 3 The PRA's duty to consult

3.1 The PRA has a statutory duty to consult when introducing new rules and, when not making rules, has a public law duty to consult widely where it would be fair to do so. When doing so, the PRA provides the following in relation to the proposed policy:

- a cost benefit analysis;
- an explanation of the PRA's reasons for believing that making the proposed policy is compatible with the PRA's duty to act in a way that advances its general objective,[22] insurance objective[23] (if applicable), and secondary competition objective;[24]
- an explanation of the PRA's reasons for believing that making the proposed policy is compatible with its duty to have regard to the regulatory principles;[25] and
- a statement as to whether the impact of the proposed policy will be significantly different to mutuals than to other persons.[26]

3.2 The Prudential Regulation Committee (PRC) should have regard to aspects of the Government's economic policy as recommended by HM Treasury.[27]

3.3 The PRA is also required by the Equality Act 2010[28] to have due regard to the need to eliminate discrimination and to promote equality of opportunity in carrying out its policies, services and functions.

## Cost benefit analysis

3.4 The proposals in this CP either:

22 Section 2B of FSMA.
23 Section 2C of FSMA.
24 Section 2H(1) of FSMA.
25 Sections 2H(2) and 3B of FSMA.
26 Section 138K of FSMA.
27 Section 30B of the Bank of England Act 1998.
28 Section 149.

- build on existing regulatory requirements such as MODR or the Solvency II Commission Delegated Regulation;

- complement the proposals on operational resilience in CP29/19; or

- seek to implement the EBA Outsourcing Guidelines and have regard to the draft EIOPA Cloud Outsourcing Guidelines.

3.5 The PRA does not expect firms to incur significant additional costs as a result of the proposals set out in this Consultation Paper.

3.6 The proposals in this CP help strengthen firms' oversight of third parties and, by doing so, help improve their operational resilience. In turn, this should improve firms' ability to anticipate, prevent, mitigate, respond to and recover from operational outages. Strengthening firms' operational resilience will also help to limit any potential adverse consequences for financial stability caused by operational outages at key outsource providers.

## Compatibility with the PRA's objectives

3.7 The proposals in this CP seek to modernise and strengthen the regulation of outsourcing and third party risk management. In light of firms' increasing reliance on third parties and the growing focus and evolving PRA policy on operational resilience, the proposals in this CP should help promote the safety and soundness of firms by improving their governance, risk management and oversight of third parties. In the case of insurers, the proposals in this CP should help secure an appropriate degree of protection for policyholders by, for instance, clarifying the PRA's expectations on the protection of confidential and sensitive data outsourced to third parties.

3.8 The PRA has assessed whether the proposals in this CP facilitate effective competition. Outsourcing, particularly to the Cloud, can be cheaper, more secure and offer flexibility for smaller firms. By providing firms with access to flexible and agile infrastructure, outsourcing has the potential to reduce barriers to entry for those firms who may not be able to invest in their own solutions. The 'Future of Finance' report identified that a lack of clear regulatory expectations has the potential to stifle the adoption of outsourcing. Therefore, clarifying the PRA's expectations on outsourcing generally and how smaller firms can comply proportionately may facilitate effective competition by lowering firms' operating costs and reducing barriers to entry.

## Regulatory principles

3.9 In developing the proposals in this CP, the PRA has had regard to the regulatory principles. Three of the principles are of particular relevance:

(iii) The principle that a burden or restriction which is imposed on a person should be proportionate to the benefits which are expected to result from the imposition of that burden. The PRA has followed this principle when developing the proposals outlined in this CP, and has indicated in the CP the key areas of its judgements. For instance, by applying the principle of proportionality to the proposals in this CP and signposting where it may apply in practice, coupled with the proposal to limit the application of the most detailed expectations only to material outsourcing arrangements.

(iv) The need to use the resources of the PRA in the most efficient and economic way. The PRA has followed this principle by, for instance, anchoring its expectations on existing requirements where possible and only building on them where deemed appropriate . The proposed creation of an online portal for firms to submit the information required by the Outsourcing Register also

seeks to promote an efficient use of the PRA's time and resources by standardising the way in which data is submitted to the PRA and optimising the tools to analyse and compare this data.

(v) The principle of senior management responsibility in firms. Chapter 4 of the draft SS in particular underscores the role of the board and senior management, including individuals performing Senior Management Functions (SMFs) under the Senior Managers and Certification Regime (SM&CR) in meeting the proposed expectations.

## Impact on mutuals

3.10 The PRA considers that the impact of the proposals in this CP on mutuals is expected to be no different from the impact on other firms. The application of the principle of proportionality to the proposals in this CP should ensure an implementation that is consistent with the characteristics and risk profile of mutuals. Moreover, the exclusion of credit unions and NDFs from the majority of the detailed proposals in this CP is also designed to ensure proportionality for smaller, less complex institutions including mutuals.

## HM Treasury recommendation letter

3.11 HM Treasury has made recommendations to the PRC about aspects of the Government's economic policy to which the PRC should have regard when considering how to advance the PRA's objectives and apply the regulatory principles.[29]

3.12 The aspects of the Government's economic policy most relevant to the proposals in this CP are Competition and Innovation.

3.13 Competition has been considered in the 'compatibility with the PRA's objectives' and 'regulatory principles' sections above.

3.14 The proposals in this CP seek to modernise the regulation of third-party risk management and are partly a response to evolving business models and industry practices which place increasing reliance on technology provided by third parties. A key driver of these industry changes is innovation.

3.15 By clarifying and enhancing regulatory expectations in areas such as Cloud outsourcing, the proposals in this CP should promote innovation in a manner consistent with the PRA's objectives.

29 Information about the PRC and the recommendations from HM Treasury are available on the Bank's website at https://www.bankofengland.co.uk/about/people/prudential-regulation-committee.

# Appendix: Draft supervisory statement – Outsourcing and third party risk management

## 1 Introduction

1.1 This supervisory statement (SS) sets out the Prudential Regulation Authority's (PRA) expectations of how PRA-regulated firms should comply with regulatory requirements and expectations relating to outsourcing and third party risk management. In particular:

- Chapter 2 elaborates on the definition of 'outsourcing' in the PRA Rulebook. It also notes that there are arrangements between firms and third parties that fall outside this definition ('third party arrangements') and are, consequently outside of scope of existing requirements on outsourcing and many of the detailed expectations in this SS. However, these third party arrangements are still subject to the PRA Fundamental Rules (FRs) and other PRA requirements and expectations on business continuity, governance, operational resilience and risk management.[1]

- Chapter 3 clarifies how the principle of proportionality applies to the expectations in this SS. In particular, to intra-group outsourcing and to 'non-significant firms' (as defined in paragraph 3.9 of this SS).

- Chapter 4 sets out the PRA's expectations on:

    - governance, including under the Senior Managers and Certification Regime (SM&CR); and

    - record keeping, in particular regarding the register of outsourcing arrangements ('Outsourcing Register'). The Appendix contains guidance for firms on how to complete the Outsourcing Register.

- Chapter 5 highlights the PRA's expectations during the pre-outsourcing phase. In particular, in relation to due diligence, the assessment of outsourcing arrangements' materiality (including notification to the PRA where required) and the risk assessment.

- Chapter 6 lists the areas which the PRA expects written agreements relating to material outsourcing to address as a minimum. The following four areas are then examined in detail in chapters 7-10:

    - data security (Chapter 7);

    - access, audit and information rights (Chapter 8);

    - sub-outsourcing (Chapter 9); and

    - business continuity and exit strategies (Chapter 10).

1.2 This SS is relevant to all:

---

1 At the time of publication of this draft SS for consultation, the proposed requirements on Operational Resilience were also out for consultation. Subject to the outcome of both consultations, the PRA may amend references to the Operational Resilience requirements and expectations in this draft SS. These references are in square brackets in this draft SS.

- UK banks, building societies and PRA-designated investment firms (hereafter 'banks');
- insurance and reinsurance firms and groups in scope of Solvency II, including the Society of Lloyd's and managing agents (hereafter 'insurers'); and
- UK branches of overseas banks and insurers (hereafter 'third-country branches'). Entities in scope of this SS are collectively referred to as 'firms'.

1.3 Some of the requirements and expectations referred to in this SS also apply to credit unions and non-directive firms (NDFs). In particular, paragraph 1.8, the requirements in Table 2; paragraphs 5.11-5.12 and the PRA statutory powers and requirements in Tables 6 and 7. The remaining expectations in this SS do not apply to credit unions and NDFs.

1.4 The aims of this SS are to:

- Complement the requirements and expectations on operational resilience [in the PRA Rulebook; SSxx/20 'Operational resilience: Impact tolerances for important business services'; and PRA Statement of Policy (SoP) on operational resilience];[2]
- 'Facilitate greater resilience and adoption of the cloud and other new technologies' as set out in the Bank of England (the Bank)'s response to the 'Future of Finance' report.[3]
- Implement the:
    - European Banking Authority (EBA) 'Guidelines on Outsourcing Arrangements' (EBA Outsourcing Guidelines). The SS clarifies how the PRA expects banks to approach the EBA Outsourcing Guidelines in the context of its requirements and expectations. In addition, certain chapters in the SS expand on the expectations in the EBA Outsourcing Guidelines. For instance, Chapters 7 (Data Security) and 10 (Business Continuity and exit plans).[4] [5]
- Take into account the:
    - draft European Insurance and Occupational Pensions Authority (EIOPA) 'Guidelines on Outsourcing to Cloud Service Providers' (EIOPA Cloud Guidelines).[6]
    - Relevant sections of the EBA Guidelines on ICT and security risk management (EBA ICT Guidelines).[7]

1.5 To promote consistency across PRA-regulated firms, the expectations in this SS apply to all forms of outsourcing and, where indicated, other third party arrangements entered into by banks and

---

2 Available in draft within CP29/19 at: 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 https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.
5 Ther terms contingency and continuity plan stem from European legislation. They are used interchangeably in this SS.
6 https://eiopa.europa.eu/Publications/Consultations/2019-07-01%20ConsultationDraftGuidelinesOutsourcingCloudServiceProviders.pdf. At the time of publication of this draft SS for consultation, the draft EIOPA Cloud Guidelines had not been finalised. Subject to the final form of these Guidelines, the final version of this SS may be updated accordingly.
7 https://eba.europa.eu/documents/10180/2522896/EBA+BS+2018+431+%28Draft+CP+on+Guidelines+on+ICT+and+security+risk+management%29.pdf.

insurers. However, this SS includes specific examples, references and even chapters (eg Chapter 7) which aim to address the specific characteristics of Cloud usage and set out conditions that can help give firms assurance and deploy it 'in a safe and resilient manner'.[8] In developing the expectations in this SS, including in relation to Cloud, the PRA has taken into account international standards, such as the 'G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector' (G-7 Third-Party Elements).[9]

1.6 To promote clarity and certainty, this SS includes references to other regulatory requirements that govern outsourcing by firms. Firms are required to comply with the obligations in these sources. This SS should therefore be read alongside and interpreted consistently with all relevant sources of law, including those in Tables 1 and 2.

**Table 1: Existing requirements and expectations on outsourcing for banks and insurers**

| Banks | Insurers |
|---|---|
| MiFID II Directive: Article 16(5) | Solvency II Directive: Articles 34(5), 38, 41(3), 49 |
| Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II [10] ('MODR'), Articles 30-32 | Commission Delegated Regulation (EU) 2015/35 supplementing Solvency II ('delegated Act').[11] Articles 274 and 294(8) |
| CRDIV Article 74 | |
| Outsourcing Part of the PRA Rulebook and Chapter 7 of the Internal Governance of Third-Country Branches Part of the PRA Rulebook | Chapter 7 of the Conditions Governing Business Part of the PRA Rulebook |
| Chapters 4.1(21) (banks) of the Allocation of Responsibilities and 3.1(A3)(12) of the Insurance-Allocation of Responsibilities Parts of the PRA Rulebook | Rule 3.1(12) of the Insurance – Allocation of Responsibilities Part of the PRA Rulebook |
| Chapter 2.3(1)(e) of the Notification Part of the PRA Rulebook | Rule 2.3(1)(e) of the Insurance- Notification Part of the PRA Rulebook |
| Rules 2.2 and 3.3 of the Information Gathering Part of the PRA Rulebook | Rule 2.2 and 3.3 of the Information Gathering Part of the PRA Rulebook |
| Rules 3.2 and 3.4 of the Operational Continuity Part of the PRA Rulebook | |
| [Rules 2.5 and 4.1 of the Operational Resilience Part of the PRA Rulebook ][12] | [Rules 2.5 and 4.1 of the Insurance – Operational Resilience Part of the PRA Rulebook] |
| EBA Outsourcing Guidelines | |
| Chapters 9 and 12 of the Ring-Fenced Bodies Part of the PRA Rulebook (only applicable to ring-fenced bodies as defined in Section 417 of FSMA) | |
| EBA Guidelines on Internal Governance (EBA Governance Guidelines) | EIOPA Guidelines on the System of Governance[13] Guidelines 14 and 60-64 |
| EBA Recommendations on Outsourcing to Cloud Service Providers (EBA Cloud Recommendations) until superseded by the EBA Outsourcing Guidelines | draft [EIOPA Cloud Guidelines (see Footnote 5)] |
| SS28/15 'Strengthening individual accountability in banking'[14] paragraphs 2.11-G, 2.41A | SS35/15 'Strengthening individual accountability in insurance'[15] paragraphs 2.22A, 2.22L, 2.31, 2.33, 2.37A, 2.37B, 2.40, 2.52, 2.93 |

8 https://www.bankofengland.co.uk/research/future-finance.
9 https://www.fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf.
10 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0565.
11 http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/77749/03-07-2019.
12 References to the Operational Resilience/Insurance Operational Resilience parts of the Rulebook and the SoP on Operational Resilience are subject to the outcome of the consultation on CP29/19.
13 https://eiopaeuropa.eu/guidelinessii/eiopa_guidelines_on_system_of_governance_en.pdf.
14 July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss.
15 July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-insurance-ss.

| | |
|---|---|
| SS21/15 'Internal Governance'[16] paragraphs 2.15, 2.23 | |
| SS9/16 'Ensuring operational continuity in resolution'[17] paragraphs 2.1, 5.1, 5.10, 6.1, 8.2, 11.5, and Chapter 4. | |
| [SS29/19 'Operational resilience: Impact tolerances for important business services'] | |
| [PRA Statement of Policy (SoP) on Operational Resilience] | |

1.7 The PRA also expects firms to interpret this SS consistently with all relevant Financial Conduct Authority (FCA) rules and guidance for dual-regulated firms, including on operational resilience. The FCA's rules and guidance on outsourcing and third party risk management are substantively aligned to the equivalent PRA requirements and expectations in Tables 1 and 2, and set out mainly in the Systems and Controls (SYSC) Sourcebook of the FCA Handbook[18] (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'.[19]

## Expectations for credit unions and non-directive firms (NDFs)

1.8 Although the majority of the detailed expectations in this SS do not apply to credit unions and NDFs, the PRA expects credit unions and NDFs to manage their outsourcing and third party arrangements prudently in a manner consistent with the PRA's objectives. The PRA will consider the extent to which they have done so when assessing their compliance with the requirements in Table 2.

**Table 2: Requirements and expectations on outsourcing for credit unions and non-directive firms**

| Credit Unions | Non-Directive Firms |
|---|---|
| Fundamental Rules | Fundamental Rules |
| Chapters 11, 13, 14, 15, 16 and 17 in the Credit Unions Part of the PRA Rulebook. | Chapters 2, 3, 4, 5, 6, 8 and 9 of the Non-Solvency II Firms – Governance Part of the PRA Rulebook |
| | Chapter 2 of the Non-Solvency II Firms – General Powers Part of the PRA Rulebook |
| Information Gathering 2.2 and 3.3 | Information Gathering 2.2 and 3.3 |
| Notifications 2.3(1)(e) | Notifications 2.3(1)(e) |
| Allocation of Responsibilities 5.2 (3),(4) and (6) | Chapter 3.1(11) of the Large Non-Solvency II Firms – Allocation of Responsibilities |
| | Non-Solvency II Firms - Allocation of Responsibilities 3.1(3) and (4) |

16 April 2017: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/internal-governance-ss.
17 July 2016: https://www.bankofengland.co.uk/prudential-regulation/publication/2016/ensuring-operational-continuity-in-resolution-ss.
18 https://www.handbook.fca.org.uk/handbook/SYSC/.
19 https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it.

# 2 Definitions and scope

## Outsourcing

2.1 The PRA Rulebook defines 'outsourcing' as 'an arrangement of any form between a firm and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be undertaken by the firm itself'. This definition derives from Article 2(3) of MODR and Article 13(28) of Solvency II.

2.2 Existing EU law, including the directly applicable requirements in Articles 30-32 of MODR and Article 274 of the Solvency II Delegated Regulation only apply to 'outsourcing' as defined in paragraph 2.1. They do not apply to other arrangements between firms and third parties which fall outside this definition. In line with the definition in the G-7 Third Party Elements and EBA ICT Guidelines, this SS defines a 'third party' as 'an organisation that has entered into a business relationship or contract with a firm to provide a product or service'.

2.3 The EBA Outsourcing Guidelines provide examples of arrangements between banks and third parties which 'as a general principle [banks] should not consider as outsourcing' (hereafter referred to as 'third party arrangements') (see paragraph 28 of the EBA Outsourcing Guidelines).

2.4 The PRA expects firms to start from the assumption that all activities, functions and services performed or provided by third parties in a 'prudential context'[20] as defined in the PRA Rulebook should come under the definition of outsourcing and, consequently, apply relevant requirements and the expectations in this SS to them, depending on their 'materiality' as discussed in Chapter 5.

## Third party arrangements - risk management

2.5 Some third party arrangements which fall outside the definition of 'outsourcing' may be relevant to the:

- financial stability of the UK;
- PRA's statutory objectives;
- operational resilience of one or more firms;
- performance of regulated activities; and/or
- Bank resolution objectives.

2.6 Examples of third party arrangements which may be relevant to the areas in paragraph 2.5 include, but are not necessarily limited, to:

- correspondent and agency banking services;

20 http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/53225/02-08-2019.

- the purchase of certain software products or technology solutions eg 'off-the shelf' machine learning (ML) models, open source software and ML libraries developed by third party providers;[21]

- the sharing of data with third parties, including through application programming interfaces (APIs) as part of Open Banking, or the purchase of data collected by third parties for analytical purposes;

- agreements between a firm and a third party to offer financial products or services (eg credit cards) using the third party's brand; and

- in the case of insurers;

    - the use of aggregators; and

    - delegated underwriting.

2.7 The PRA expects firms to have appropriate governance and internal controls to identify, manage and report risks resulting from all arrangements with third parties. Moreover, firms are reminded of the need to comply with the following requirements, which apply in respect of all third party arrangements regardless of whether they fall under the definition of outsourcing:

- the PRA FRs. In particular FRs 2, 3, 5 and 6;

- in the case of individuals, the Conduct Rules/Insurance - Conduct Standards and Senior Manager Conduct Rules/Conduct Standards;

- General Organisational Requirements 2 (banks) and Conditions Governing Business 2 (insurers). In particular, the requirements on business continuity, contingency planning and data protection;

- the Risk Control Part of the PRA Rulebook (banks) and Conditions Governing Business 3 (insurers); and

- the relevant requirements in the Operational Resilience/ Insurance – Operational Resilience parts of the Rulebook.[22]

21 See Bank of England/FCA 'Machine learning in financial services' survey, October 2019 https://www.bankofengland.co.uk/report/2019/machine-learning-in-uk-financial-services

22 Subject to the outcome of the Operational Resilience consultation.

# 3 Proportionality

3.1 The PRA expects firms to meet the expectations in this SS in a manner appropriate to their size and internal organisation and the nature, scope and complexity of their activities, in line with the principle of proportionality.

3.2 Proportionality and the materiality of outsourcing arrangements (see Chapter 5) are separate but complementary concepts, and firms should consider the links between the two. Proportionality focuses on the characteristics of a firm or group, including its systemic significance. Materiality looks at the potential impact of a given outsourcing arrangement on a firm's safety and soundness, including its operational resilience; its ability to comply with legal and regulatory obligations and (for insurers) its ability to provide an appropriate degree of protection for those who are or may become policyholders. Proportionality and materiality can change over time and firms should reassess both at appropriate, periodic intervals.

## Intra-group outsourcing

3.3 Intra-group outsourcing is subject to the same requirements and expectations as outsourcing to service providers outside a firm's group and should not be treated as being inherently less risky.

3.4 Although intra-group is subject to the same requirements as outsourcing to service providers outside a firm's group, in line with Articles 31(4) of MODR and Article 274(2), firms may comply with some of these requirements proportionately depending on their level of 'control and influence' over the group company that is providing the outsourced service. For example, they may:

- adjust their vendor due diligence;
- rely on the group's stronger negotiating and purchasing power to enter into group-wide arrangements with external parties;
- adapt certain clauses in outsourcing agreements (a written agreement is always required - see Chapter 6); or
- rely on group policies and procedures as long as they comply with their UK legal and regulatory obligations and allow them to manage relevant risks, eg group cyber-security or data protection policies.

3.5 Control and influence will vary depending on each group's corporate structure. For instance, a firm that outsources to a subsidiary is likely to have greater control and influence than one which outsources to its parent company.

3.6 When third-country branches or subsidiaries outsource to parent companies outside the UK, they should ensure that the outsourced service is provided in compliance with UK legal and regulatory requirements even if these firms are bound by policies, procedures or written agreements set by their overseas group or parent companies. They should also implement appropriate mechanisms for escalating concerns and issues with outsourced service providers, in particular those deemed material, to the group or parent.

3.7 Where relevant, firms may be able to use elements of their operational continuity in resolution (OCIR) framework in intra-group outsourcing and vice-versa. For instance, the provision of services by intra-group service companies, if clearly documented, can 'facilitate mapping of services to recipient entities and provide greater clarity about which shared services need to continue in

resolution' as well as 'the restructuring of business lines or legal entities within the group as part of resolution'.[23]

3.8 For some banks, intra-group outsourcing arrangements may be subject to the requirements in Operational Continuity Chapter 4 and Ring-Fenced Bodies chapters 9 and 12. Compliance with these requirements may also mean those banks meet certain expectations in this SS in respect of intra-group outsourcing arrangements. For instance, on business continuity and exit plans (see Chapter 10).

## Non-significant firms

3.9 The PRA Rulebook does not define a 'significant' firm. For the purposes of this SS, firms whose supervisory contact has indicated are impact category 1 or 2 should consider themselves 'significant'. This approach is consistent with the definitions of 'significant firm' in the:

- PRA Approach to Banking Supervision and PRA Approach to Insurance Supervision ('PRA Approach Documents')[24]
- EBA Outsourcing Guidelines and EBA Governance Guidelines;[25] and
- for Solvency II insurers, SS10/16.[26]

3.10 'Non-significant' firms can meet some of the expectations in this SS in a proportionate manner. The PRA's supervisory scrutiny of firms' outsourcing arrangements may also vary according to their significance.

### Governance and internal controls

3.11 Non-significant firms' business models may rely more extensively on outsourcing. However, to meet the Threshold Conditions on an ongoing basis, all firms must retain appropriate non-financial resources including to effectively oversee the outsourced services (see Chapter 4).

3.12 An example of a function which non-significant firms can outsource is internal audit. Firms that elect to do so are not required to have an individual approved as the Head of Internal Audit Senior Management Function (SMF5) under the SM&CR but must allocate a Prescribed Responsibility for overseeing the provision of the outsourced internal audit function to another existing SMF (see Allocation of Responsibilities 4.2(3) (banks) and Insurance – Allocation of Responsibilities 3.3 (insurers)).

3.13 While all firms should have appropriate non-financial resources to oversee their outsourcing arrangements, individuals across business lines and internal control functions responsible for doing so in non-significant firms may be less specialised and have general responsibility for areas such as compliance, IT or risk management.

---

23 See Financial Stability Board, *Guidance on Arrangements to Support Operational Continuity in Resolution*, 18 August 2016: https://www.fsb.org/wp-content/uploads/Guidance-on-Arrangements-to-Support-Operational-Continuity-in-Resolution1.pdf.

24 Available at: https://www.bankofengland.co.uk/prudential-regulation/publication/pras-approach-to-supervision-of-the-banking-and-insurance-sectors.

25 Institutions referred to in Article 131 of CRDIV (global systemically important institutions (G-SIIs) and other systemically important institutions (O-SIIs)), and, as appropriate, other institutions determined by the competent authority or national law, based on an assessment of the institutions' size and internal organisation, and the nature, scope and complexity of their activities.

26 See paragraph 1.2 of SS10/16 'Solvency II: Remuneration requirements', July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2016/solvency-2-remuneration-requirements-ss

3.14 Although non-significant firms' outsourcing policies should include the minimum requirements in Chapter 4, the length and complexity of their policies may reflect the complexity, materiality and number of the firm's outsourcing relationships.

## Access, audit and information rights

3.15 Although all firms are in principle able to use the access, audit and information-gathering methods highlighted in Chapter 7, including third party certification and pooled audits, these methods may allow non-significant firms to mitigate the cost and resource implications of conducting individual onsite audits. However, non-significant firms should still be satisfied that whichever method they use allows them to meet their individual legal and regulatory obligations, and align to their risk appetite.

# 4 Governance and record-keeping

4.1 This chapter sets out the PRA's expectations on:

- board engagement on outsourcing;
- outsourcing and the Senior Managers and Certification Regime (SM&CR);
- outsourcing policies; and
- record keeping; in particular regarding the Outsourcing Register.

4.2 In this chapter, the term 'board' encompasses the terms 'governing body' and 'management body' in the PRA Rulebook and refers to the board of directors or equivalent body in a firm.

## Governance

### Board engagement on outsourcing

4.3 Boards and senior management, in particular individuals performing Senior Management Functions (SMFs), cannot outsource their responsibilities. Firms that enter into outsourcing arrangements remain fully accountable for complying with all their regulatory obligations. This is a key principle underlying all requirements and expectations regarding outsourcing, including the expectations in this SS.

4.4 Firms' boards should:

- set 'the control environment throughout the firm, including the appetite and tolerance levels in respect of outsourcing risk';
- 'bear responsibility for the effective management of all risks to which the firm is exposed' including by:
    - appropriately 'identifying and understanding of the firm's reliance on critical service providers'; and
    - ensuring that the firm has '(from board level downwards) appropriate and effective risk management systems and strategies in place to deal with outsourced service providers'.[27]

4.5 In line with SS5/16, the PRA expects management information on outsourcing provided to the board to be clear, consistent, robust, timely, well-targeted and contain an appropriate level of technical detail to facilitate effective oversight and challenge by the board.[28]

### Empty shells

4.6 Firms should avoid becoming 'empty shells' (as mentioned in the EBA Outsourcing Guidelines) which are incapable of meeting the Threshold Conditions (TCs). The following TCs are particularly relevant :

---

27 These principles were outlined in Final Notice, R. Raphaels & Sons, 29 May 2019: https://www.bankofengland.co.uk/news/2019/may/fca-and-pra-jointly-fine-raphaels-bank-1-89m-for-outsourcing-failings

28 SS5/16 'Corporate Governance: Board responsibilities', July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2016/corporate-governance-board-responsibilities-ss.

- being capable of being effectively supervised by the PRA;

- the 'suitability' threshold condition in Sections 4E (Part1A) (insurers) and 5E (Part 1E) (banks) of FSMA. In line with the EBA Outsourcing Guidelines, this should include retaining 'a clear and transparent organisational framework and structure'; and

- conducting their business in a prudent manner, including having appropriate non-financial (as well as financial) resources.

## Outsourcing and the SM&CR

4.7 Allocation of Responsibilities 4.1(21) (banks) and Insurance-Allocation of Responsibilities 3.1(A3)(12) (insurers) require firms to allocate a Prescribed Responsibility for a firm's regulatory obligations in relation to outsourcing to an SMF.

4.8 Depending on the size and complexity of the firm and the SMFs it requires, the PRA expects but does not require this Prescribed Responsibility to be allocated to (one of) the individuals performing the Chief Operations Senior Management Function (SMF24) (which, as noted in SS28/15 for banks and SS35/15 for insurers can be split among more than one individual in certain circumstances). SMF24s may also be responsible for other areas or activities relevant to the expectations in this SS, such as the firm's information security policy.

4.9 Firms should interpret this Prescribed Responsibility as encompassing the firm's overall framework, policy and systems and controls relating to outsourcing. Responsibility for individual outsourcing arrangements may still lie with relevant business lines. The free text section of the relevant SMF's Statement of Responsibilities should describe this responsibility in an appropriate level of detail in line with SS28/15.

## Outsourcing Policy

4.10 The EBA Outsourcing Guidelines and EBA Governance Guidelines (banks); and conditions Governing Business 2.4(1) (insurers) state that firms' boards should approve, regularly review and implement a written outsourcing policy. Firms may elect to apply this policy or parts thereof to all third-party arrangements. This policy should align to and draw upon other relevant firm policies and strategies. For instance:

- business model and strategy;

- business continuity;

- conflicts of interest;

- data protection;

- information and communications technology (ICT);

- information security;

- operational resilience;

- OCIR;

- (if applicable) ring-fencing; and

- risk management.

4.11 Firms should make outsourced and third party providers aware of relevant internal policies eg on outsourcing, ICT, information security or operational resilience.

4.12 As discussed further in Chapter 10, firms' business continuity plans under General Organisational Requirements 2.5 and 2.6 (banks) and Conditions Governing Business 2.6 (insurers) should take into account:

- the possibility that the quality of the provision of material outsourced services deteriorates to unacceptable levels;

- the potential impact of the insolvency or other failure of the service provider or the failure of the service (see Chapter 10); and

- where relevant, political and other risks in the service provider's jurisdiction.

4.13 There is no 'one-size-fits-all' template for firms' outsourcing policies. Firms and groups are responsible for developing and maintaining a policy that is appropriate to their complexity, organisational structure and size (see Chapter 3).

4.14 The outsourcing policy should be principles-based and may be supported by detailed procedures developed, approved and maintained below board level. However, it should be sufficiently detailed to provide adequate 'guidance for firms' staff on how to apply [its] requirements in practice'. At a minimum, it should cover the areas in Table 3.

**Table 3: Contents of the outsourcing policy**

| | |
|---|---|
| General | The responsibilities of the board, including its involvement, as appropriate, in decisions about material outsourcing.<br><br>The involvement of business lines, internal control functions and other individuals (in particular, SMFs) in respect of outsourcing arrangements.[29]<br><br>Links to other relevant policies (see paragraph 4.8).<br><br>Documentation and record-keeping.<br><br>Procedures for the identification, assessment, management and mitigation of potential relevant conflicts of interest.[30]<br><br>Business continuity planning (BCP) (see paragraph 4.9).<br><br>Differences, if any, between the approach to:<br>- intra-group outsourcing vs outsourcing to external service providers;<br>- material vs non-material outsourcing;<br>- outsourcing to service providers regulated or overseen by the Bank, PRA or FCA vs unregulated service providers; and<br>- outsourcing to service providers in specific jurisdictions outside the UK. |
| Pre-outsourcing & on-boarding | The processes for vendor due diligence and for assessing the materiality and risks of outsourcing arrangements (including notification to the PRA where required). |

29 See paras. 50-51 of the EBA Outsourcing Guidelines in respect of the role of the internal audit function in particular.
30 See paras 45-47 of the EBA Outsourcing Guidelines

| | |
|---|---|
| | Responsibility for signing-off new outsourcing arrangements. In particular material outsourcing arrangements. |
| Oversight | Procedures for the ongoing assessment of service providers' performance including where appropriate:<br>- day-to-day oversight, including incident reporting; periodic performance assessment against service level agreements; and periodic strategic assessments;<br>- being notified and responding to changes to an outsourcing arrangement or service provider (eg to its financial position, organisational or ownership structures, sub-outsourcing);<br>- independent review and audit of compliance with legal and regulatory requirements and policies; and<br>- renewal processes. |
| Termination | Exit strategies and termination processes, including a requirement for a documented exit plan for material outsourcing arrangement where such an exit is considered possible taking into account possible service interruptions (and the firm's impact tolerance for important business services) or the unexpected termination of an outsourcing agreement (see Chapter 10) |

## Record-keeping

4.15 From 31 December 2021, the EBA Outsourcing Guidelines expect banks to maintain an up-to-date register of information on all their outsourcing arrangements distinguishing between those which are material and those which are not ('Outsourcing Register').

4.16 More specifically, the EBA Outsourcing Guidelines expect that firms should start populating the Outsourcing Register with any new outsourcing arrangements entered into from 30 September 2019, while progressively adding outsourcing arrangements entered into before 30 September 2019 with a view to having a complete Outsourcing Register by 31 December 2021.

4.17 Banks are already expected to maintain a register of their Cloud outsourcing arrangements ('Cloud Register') in line with the EBA Cloud Recommendations. Banks are expected to continue to maintain the Cloud Register until the Outsourcing Register subsumes it by 31 December 2021.

4.18 The Appendix to this SS sets out information on how firms should consistently fill in the qualitative data fields that the EBA Outsourcing Guidelines provide should be included in the Outsourcing Register. This Appendix is also applicable to the Cloud Register until that is subsumed.

# 5 Pre-outsourcing phase

5.1 The PRA expects firms to:

- determine the materiality of every outsourcing arrangement;
- perform appropriate and proportionate due diligence on all potential service providers; and
- assess the risks of every outsourcing arrangement irrespective of materiality.

## Materiality assessment

### Definition

5.2 The PRA Rulebook defines 'material outsourcing' as the outsourcing of 'services of such importance that weakness, or failure, of the services would cast serious doubt upon the firm's continuing satisfaction of the threshold conditions or compliance with the Fundamental Rules'.[31]

5.3 Materiality should be read as incorporating the concept of a 'critical or important operational function' in relevant EU law provisions. The requirements in Article 31 of MODR or Article 274(5) of the delegated Act apply only to the outsourcing of critical or important operational functions.

5.4 This SS uses 'material outsourcing' instead of 'critical or important' for clarity and to avoid confusion with different but partly overlapping terms such as 'critical function' or 'critical service' in an OCIR context.

5.5 As the definition of materiality is tied to an individual firm's ability to meet the TCs on an ongoing basis and comply with the FRs, materiality should be assessed at an individual firm level. Where a group or parent company assesses the materiality of an outsourcing arrangement on the group as a whole, individual firms may rely on information and findings from the group-wide assessment but should still take reasonable steps to come to an informed view as to the materiality of the arrangement on them as an individual firm.

### Timing and frequency of materiality assessments

5.6 Firms are responsible for assessing the materiality of their outsourcing arrangements. Materiality may vary throughout the duration of an arrangement and should therefore be (re)assessed:

- prior to signing the written agreement;
- at appropriate intervals thereafter eg during scheduled review periods;
- where a firm plans to scale up its use of the service or dependency on the service provider; and/or
- if an organisational change at the service provider or a material sub-outsourced service provider takes place, including a change of ownership or to their financial position.

---

31 See the Notifications 2.3(e) part of the PRA Rulebook: http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/52175/12-06 2019.

5.7 Where a firm expects an outsourcing arrangement to become material in the future, it should take reasonable steps to ensure that it can comply with the expectations for material outsourcing arrangements in chapters 6 to 10 on or before the materiality threshold is crossed.

## Criteria for assessing materiality

5.8 Firms should develop their own processes for assessing materiality as part of their outsourcing policy (see Chapter 4). However, to ensure consistency across firms' assessments, the PRA expects firms to take into account certain criteria.

### *Criteria that will generally render an outsourcing arrangement automatically material*

5.9 Consistent with the definition of 'material outsourcing' in the PRA Rulebook and, where applicable, the criteria in the EBA Outsourcing Guidelines, a firm should generally consider an outsourcing arrangement as material where a defect or failure in its performance could materially impair the:

- financial stability of the UK;
- firm's:
    - ability to meet the TCs;
    - compliance with the FRs;
    - requirements under 'relevant legislation' and the PRA Rulebook;[32]
    - safety and soundness, including its:
        - (i) financial resilience, ie assets, capital, funding and liquidity; or
        - (ii) operational resilience, ie its ability to continue providing important business services.
    - for insurers only, the:
        - ability to provide an appropriate degree of protection for those who are or may become policyholders in line with the PRA's statutory objectives; and
        - requirement not to undermine the 'continuous and satisfactory service to policy holders' in line with Article 49(2)(c) of Solvency II.
    - OCIR and resolvability, if applicable.

5.10 The PRA also expects firms to classify an outsourcing arrangement as material if the service being outsourced involves an:

---

32 Defined as FSMA; the Capital Requirements Regulations (CRR); the Solvency 2 Regulations 2015; any other enactment; or any directly applicable EU regulation http://www.prarulebook.co.uk/rulebook/Content/Part/211407/26-06-2019

- entire 'regulated activity', eg accepting deposits or effecting a contract of insurance as principal;[33] or

- 'internal control'[34] or 'key function'[35] unless the firm is satisfied that a defect or failure in performance would not adversely affect the relevant function.

### *Other materiality criteria to take into account*

5.11 The PRA expects firms to have regards to all applicable criteria in Table 4, both individually and in conjunction when assessing the materiality of an outsourcing arrangement not otherwise covered by paragraphs 5.8 and 5.9.

**Table 4: Materiality criteria**

| | |
|---|---|
| Direct connection to the performance of a regulated activity | |
| Size and complexity of relevant business area(s) or function(s) | |
| The potential impact of a disruption, failure or inadequate performance on the firm's: | business continuity, operational resilience and operational risk, including:<br>- conduct risk;<br>- information and communication technology (ICT) risk;[36]<br>- legal risk; and<br>- reputational risk.[37] |
| | ability to:<br>- comply with legal and regulatory requirements;<br>- conduct appropriate audits of the relevant function, service or service provider; and<br>- identify, monitor and manage all risks. |
| | obligations under<br>- the PRA Rulebook;<br>- the General Data Protection Regulation (GDPR);[38] and<br>- Data Protection Act 2018 (DPA).[39] |
| | counterparties, customers or policyholders. |
| | early intervention, recovery and resolution planning OCIR and resolvability. |
| The firm's ability to scale up the outsourced service. | |
| Ability to substitute the service provider or bring the outsourced service back in-house , including estimated costs, operational impact, risks and timeframe of an exit in stressed and non-stressed scenarios. | |

## Notification to the PRA

5.12 Notifications 2.3(1)(e) requires all PRA-regulated firms, including credit unions and NDFs, to notify the PRA when 'entering, or significantly changing a material outsourcing arrangement'.[40] The PRA expects these notifications to be made before entering into the outsourcing arrangement. The PRA also expects firms to submit these notifications before an outsourcing arrangement that was

33 See also paras.62 and 63 of the EBA Outsourcing Guidelines regarding the outsourcing of entire regulated (banking) activities to service providers located outside the EEA.
34 http://www.prarulebook.co.uk/rulebook/Glossary/Rulebook/0/17-06-2019/I
35 http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/52841/17-06-2019
36 As defined in the EBA *Guidelines on ICT and security risk management*
37 In line with the definition of *operational risk* in Articles 13(33) and Art. 101(4) of Solvency II Directive and the PRA Rulebook, http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/52863/24-06-2019, insurers should consider reputational risks in addition to and separately from operational risk.
38 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en
39 https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf
40 http://www.prarulebook.co.uk/rulebook/Content/Chapter/211501/17-06-2019

not initially deemed material is expected or planned to become so (see paragraph 5.5). The PRA will consider the timeliness of these notifications when assessing firms' compliance with FR 7.

5.13 The PRA expects firms to assess the materiality of planned outsourcing arrangements sufficiently early to notify the PRA if required and:

- provide additional information if requested to do so; and
- implement follow-up action if appropriate, which may involve a firm:
    - enhancing its due diligence, governance or risk management and delaying entering into the agreement until it does so; or
    - reviewing the written agreement to ensure it complies with their regulatory obligations and risk management expectations (see Chapter 6).

5.14 The PRA expects notifications of material outsourcing to include, at least, the information in paragraph 54 of the EBA Outsourcing Guidelines.

### Due diligence

5.15 Before entering into an outsourcing arrangement, the PRA expects firms to conduct appropriate due diligence on potential service providers, including the identification of possible alternative or back-up providers.

5.16 In the case of material outsourcing, the PRA expects firms' due diligence to consider the potential providers':

- business model, complexity, financial situation, nature, ownership structure, and scale;
- capability, expertise, and reputation;
- financial, human, and technology resources
- IT and cyber security controls; and
- any sub-outsourced service providers that will be involved in the delivery of important business services or parts thereof.

5.17 The due diligence should also consider whether potential service providers:

- have the authorisations or registrations required to perform the service;
- comply with the GDPR, DPA and other applicable legal and regulatory requirements on data protection; and
- can demonstrate certified adherence to recognised, relevant industry standards.

## Risk assessment

5.18 In line with Risk Control 3.4(2) of the PRA Rulebook,[41] firms should assess the potential risks of all third party arrangements, including outsourcing arrangements regardless of materiality. Firms

41 http://www.prarulebook.co.uk/rulebook/Content/Chapter/214204/04-12-2019

may, however, carry out a proportionate risk assessment in the case of non-material arrangements. As part of the risk assessment, the PRA expects firms to consider:

- operational risks based on an analysis of severe but plausible scenarios. For instance, a breach or outage affecting the confidentiality, integrity and availability of sensitive data (see Chapter 10);[42] and,

- financial risks, including the potential need for the firm to provide financial support to a material outsourced or sub-outsourced service provider in distress or take over its business ('step-in' risk).[43]

### Timing and frequency of risk assessments

5.19 The PRA expects firms to carry out risk assessments in the circumstances referred to in paragraph 5.6 and also if they consider that there may have been a significant change to an outsourcing arrangement's risks due to, for instance, a serious breach/continued breaches of the agreement or a crystallised risk.

### Benefits of the outsourcing arrangement and risk mitigation

5.20 A firm's risk assessment should balance any risks which the outsourcing arrangement may create or increase against any risks it may reduce or enable the firm to manage more effectively. For instance, a firm's resilience to disruption. The assessment should also take into account existing or planned risk mitigation, eg staff procedures and training.

### Firm or group-wide concentration risk

5.21 The PRA expects firms and groups to periodically (re)assess and take reasonable steps to manage:

- their overall reliance on third parties; and

- concentration risks or vendor lock-in at the firm or group, due to:

    - multiple arrangements with the same or closely connected service providers; or

    - arrangements with service providers that are difficult or impossible to substitute.

42 http://www.prarulebook.co.uk/rulebook/Content/Chapter/211209/17-06-2019; http://www.prarulebook.co.uk/rulebook/Glossary/FullDefinition/52863/17-06-2019

43 See BCBS Guidelines on identification and management of step-in risk, 25 October 2017: https://www.bis.org/bcbs/publ/d423.pdf.

# 6 Outsourcing agreements

6.1 In line with Article 31(3) of MODR (banks) and 274(3)(c) of the delegated Act (insurers), all outsourcing arrangements must be set out in a written agreement.

6.2 Where there is a master service agreement that allows firms to add or remove certain services, the PRA expects every individual outsourced service to be appropriately documented, although not necessarily in a separate agreement and recorded in the Outsourcing Register.

6.3 In relation to written agreements for non-material outsourcing arrangements firms should agree appropriate contractual safeguards to manage relevant risks. However, regardless of materiality, firms should ensure that outsourcing agreements do not impede or limit the PRA's ability to effectively supervise the firm or outsourced activity, function or service.

6.4 The remainder of this chapter lists the areas which the PRA expects written agreements for material outsourcing to address as a minimum. Chapters 7-10 cover the following four areas in detail:

- data security (chapter 7);
- access, audit, and Information rights (chapter 8);
- sub-outsourcing (chapter 9); and
- business continuity and exit plans (chapter 10).

## Material outsourcing agreements

6.5 Written agreements for material outsourcing should set out at least:

- a clear description of the outsourced function, including the type of support services;
- the start date, next renewal date, end date and notice periods regarding termination for the service provider and the firm;
- the court jurisdiction and governing law of the agreement;
- the parties' financial obligations;
- whether the sub-outsourcing of a material function or part thereof is permitted and, if so, under which conditions;
- the location(s), ie regions or countries where the material function or service will be provided, and/or where relevant data will be kept and stored, processed or transferred, including a requirement for the service provider to notify the firm in advance if it proposes to change said location(s);
- provisions regarding the accessibility, availability, integrity, confidentiality, privacy, and safety of relevant data (see Chapter 7);
- the right of the firm to monitor the service provider's performance on an ongoing basis (by reference to key performance indicators (KPIs));

- the agreed service levels, which should include qualitative and quantitative performance criteria and allow for timely monitoring, so that appropriate corrective action can be taken if these service levels are not met;

- the reporting obligations of the service provider to the firm, including a requirement to notify the firm of any development that may have a material impact on the service provider's ability to effectively perform the material function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements;

- whether the service provider should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;

- the requirements for both parties to implement and test business contingency plans, which should take account of firms' impact tolerances for important business services. This should include a commitment on both parties to support the testing of such plans;

- provisions to ensure that data owned by the firm can be accessed promptly in the case of the insolvency, resolution or discontinuation of business operations of the service provider;

- the obligation of the service provider to co-operate with the PRA and the Bank, as resolution authority, including persons appointed to act on their behalf (see Chapter 8, including the section on the Bank's and PRA's information-gathering and investigatory powers);

- for banks, a clear reference to the Bank's resolution powers especially under Sections 48Z and 70C-D of the Banking Act 2009 (implementing Articles 68 and 71 of Directive 2014/59/EU (BRRD)), and in particular, a description of the 'substantive obligations' of the written agreement in the sense of Article 68 of that Directive);

- the rights of firms and the PRA to inspect and audit the service provider with regard to the material outsourced function (see Chapter 8);

- if relevant,

    - appropriate and proportionate information security related objectives and measures including requirements such as minimum cybersecurity requirements, specifications of firms' data life cycle, and any requirements regarding to data security (see Chapter 7), network security and security monitoring processes; and

    - operational and security incident handling procedures including escalation and reporting; and

- termination rights and exit strategies covering both stressed and non-stressed scenarios, as specified in Chapter 10. As in the case of business contingency plans, both parties should commit to take reasonable steps to support the testing of firms' termination plans.

# 7 Data security

7.1 In this chapter, the term 'data' should be interpreted broadly to include confidential, firm, sensitive and transactional data as well as the systems used to process, transfer or store data.

7.2 Where a material outsourcing agreement involves the transfer of data, the PRA expects firms to define, document and understand their and the service provider's respective responsibilities in respect of that data and take appropriate measures to protect them. The term commonly used to help firms and Cloud providers understand their respective obligations is the 'shared responsibility model'.

7.3 Table 5 sets out an example of how the shared responsibility model operates in the case of data outsourced to Cloud service providers.

**Table 5: The Shared responsibility model in Cloud outsourcing**

| Cloud |
| --- |
| Cloud service providers tend to operate under the 'shared responsibility model' whereby:<br><br>the firm is responsible for what's in the Cloud and the Cloud service provider is responsible for the provision of the Cloud.<br><br>firms remain responsible for correctly identifying and classifying data in line with their legal and regulatory obligations and determining which jurisdictions certain data can be stored in or routed through (data location). They also remain responsible for configuration and monitoring of their data in the Cloud to reduce security and compliance incidents;<br><br>Cloud service providers assume responsibility for the infrastructure running the outsourced service eg data centres, hardware, software etc.; and<br><br>firms and service providers share other responsibilities depending on the service model eg Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) etc.[44] |

7.4 Building on General Organisational Requirements 2.4 (banks) and Article 274(e) of the delegated Act, where a material outsourcing agreement involves the transfer of data, the PRA expects firms to:

- classify relevant data based on their confidentiality and sensitivity;
- identify potential risks relating to outsourced data and their impact (legal, reputational etc.); and
- agree an appropriate level of data availability, confidentiality and integrity.

7.5 Some risks relating to data which the PRA expects firms to consider include inappropriate access, insider threats, loss of data, unavailability of data and the unauthorised modification of data.

## Data classification

7.6 Taking into account their impact tolerances for important business services, firms' data classification should identify data which they would need to access and potentially migrate as a matter of priority in the event of disruption. This can facilitate business continuity and exit strategies as discussed in Chapter 10.

44 As defined in the EBA Outsourcing Guidelines and [draft] EIOPA Cloud guidelines.

7.7 When firms plan to outsource data to Cloud service providers, their data classification should assess the Cloud-readiness of their on-premise data and applications. In particular, when dealing with legacy infrastructure and systems.

### Data location

7.8 Firms should adopt a risk-based approach to data location, considering data-at-rest, data-in-use and data-in-transit. It should balance the:

- potential legal risks, including under GDPR, conflicting legal or regulatory requirements and challenges to firms' and the PRA's ability to access data in certain jurisdictions outside the UK (including any jurisdictions through which data may be routed) due to local law enforcement, legal or political circumstances; and

- operational resilience advantages of outsourced data being stored in multiple locations (see Chapter 10).

### Data security

7.9 The PRA expects firms to implement appropriate measures to protect outsourced data and set them out in their outsourcing policy (see Chapter 4) and written agreements for material outsourcing (see Chapter 6).

7.10 The PRA expects firms to implement robust controls for data-in-transit, data-in-memory and data-at-rest. These controls should include a mix of preventative and detective measures, including but not necessarily limited to:

- configuration management;

- encryption and key management;

- identity and access management, which should include stricter controls for individuals such as system administrators whose privileges and responsibilities can give rise to heightened risks in the event of unauthorised access;

- access and activity logging;

- incident detection and response;

- loss prevention and recovery;

- data segregation (if using a multi-tenant environment);

- operating system, network and firewall configuration;

- staff training;

- the ongoing monitoring of the effectiveness of the service provider's controls, including through the exercise of access and audit rights (see Chapter 8);

- policies and procedures to detect activities that may impact firms' information security (eg data breaches, incidents or misuse of access by third parties) and respond to these incidents

appropriately (including appropriate mechanisms for investigation and evidence collection after an incident); and

- procedures for the deletion of firm data from all the locations where the service provider may have stored it following an exit or termination, and provided that access to the data by the firm or PRA is no longer required (see chapters 8 and 10).

7.11 Where data is encrypted, firms should ensure that any encryption keys or other forms of authentication are kept secure and accessible to the PRA in accordance with FR 7.

# 8 Access, audit and information rights

## Bank and PRA information-gathering and investigatory powers

8.1 Independent of the expectations on access, audit and information rights set out later in this chapter, the Bank and/or PRA have a range of statutory information-gathering and investigatory powers, some of which may apply directly to outsourced service providers as well as firms. The PRA expects firms to make service providers aware of the powers and requirements as set out in Tables 6 and 7 below, which are not exhaustive. However, failure to do so will not affect their applicability.

**Table 6: Bank and PRA statutory information-gathering or investigatory powers**

| Firms (All,[45] banks or insurers) | Outsourcing (all or material) | Statutory Power | Description | Directly applicable to service providers as well as firms? (Yes or No) |
|---|---|---|---|---|
| All | All | Section 165A of the Financial Services Markets Act 2000 (FSMA) | The PRA can require service providers to provide it with information it considers 'is or might be, relevant to the stability of the UK financial system.'[46] | Yes |
| All | All | Section 166(7)(b) FSMA | Any entity which is providing or has provided services to a firm in relation to matters subject to a Section 166 review must give the skilled person all such assistance as [they] may reasonably require. | Yes |
| Banks | All | Section 3A of the Banking Act 2009<br><br>(see also sections 83ZA and 83ZB of the Banking Act 2009) | The Bank as a resolution authority can direct a firm to produce information that is relevant to the exercise of its stabilisation powers and to provide that information to the Bank. | No |
| Insurers | All | Section 165(7)(e) of FSMA | The PRA can require a person who provides any service to an insurer to provide specified documents or information. | Yes |

45 The term 'All' in Tables 6 and 7 includes all PRA-regulated firms including credit unions and NDFs.
46 See Statement of Policy – The Financial Stability Information Power', June 2014: www.bankofengland.co.uk/prudential-regulation/publication/2014/the-financial-stability-information-power-sop.

**Table 7: PRA rules on access, information and audit rights**

| Firms | Outsourcing | PRA Rule | Description | Directly applicable to service providers as well as firms? (Yes or No) |
|---|---|---|---|---|
| Insurers | All | Conditions Governing Business 7.4 | Service providers must co-operate with the PRA and, where relevant, any other supervisory authority of the firm in connection with the function or activity outsourced by the firm;<br><br>The firm, its auditors, the PRA and, where relevant, other supervisory authority of the firm must have effective access to data related to the functions or activities that have been outsourced. | No |
| All | Material | Information Gathering 2.2 and 3.3 | Firms must take reasonable steps to ensure their suppliers under material outsourcing arrangements:<br>deal with the PRA in an open, co-operative and timely way in the discharge of the PRA's functions under relevant legislation; and<br>permit any representative or appointee of the PRA to have access, with or without notice, during reasonable business hours to any of its business premises, in relation to the discharge of the PRA's functions under any relevant legislation in relation to the firm. | No |

## Non-material outsourcing arrangements

8.2 The PRA expects firms to adopt a risk-based approach to access, audit and information rights in respect of non-material outsourcing arrangements. In doing so, they should take into account the arrangement's riskiness and the likelihood of it becoming material in the future (see Chapter 5).

## Material outsourcing arrangements

8.3 Building on Chapter 6, the PRA expects firms to take reasonable steps to ensure that written agreements for material outsourcing arrangements provide firms, firms' auditors, the PRA, and Bank (as a resolution authority), and any other person appointed by firms or the Bank and PRA, unrestricted access, audit and information rights to enable firms to:

- comply with their legal and regulatory obligations; and
- identify, monitor and manage risks relating to the arrangement.

8.4 Access, audit and information rights in material outsourcing arrangements should include where relevant:

- data, devices, information, systems and networks used for providing the outsourced service or monitoring its performance. This should include, where relevant, the firm's ability to carry out security penetration testing on its applications, data and systems to 'assess the effectiveness of implemented cyber and internal IT security measures and processes';
- company and financial information; and

- the service provider's external auditors, personnel and premises.

## Pooled audits and third party certificates and reports

8.5 The PRA expects firms to exercise their access, audit and information rights in respect of material outsourcing arrangements in an outcomes-focused way to assess whether the service provider is providing the relevant service effectively and in compliance with the firm's legal and regulatory obligations and expectations, including as regards operational resilience.

8.6 Firms may use a range of audit and other information gathering methods, including:

- offsite audits, such as certificates and other independent reports supplied by service providers; and

- onsite audits, either individually or in conjunction with other firms (pooled audits).

8.7 Firms can choose any appropriate audit method as long as it enables them meet their legal, regulatory, operational resilience and risk management obligations. The level of assurance expected will, however, become more onerous depending on proportionality (ie whether the firm is significant (see Chapter 3)) and the materiality of the arrangement (see Chapter 5). For instance, a significant firm which outsources an important business service for which it has set a low impact tolerance should demand a higher level of assurance.

### *Third party certificates and reports*

8.8 Certificates and reports supplied by service providers may help firms obtain assurance on the effectiveness of the service provider's controls. However, in material outsourcing arrangements, the PRA expects firms to:

- assess the adequacy of the information in these certificates and reports, and not assume that their mere existence or provision is sufficient evidence that the service is being provided in accordance with their legal, regulatory and risk management obligations; and

- ensure that certificates and reports meet the expectations in Table 8.

**Table 8: Expectations for third party certificates and audit reports**

| | |
|---|---|
| Scope | - Key systems and controls identified by the firm (eg applications, infrastructure, data centres and processes).<br>- Compliance with relevant requirements (eg PRA rules and EBA Outsourcing Guidelines). |
| Content | - Up-to-date.<br>- Reviewed regularly to reflect updates to the service provider's controls, new or revised legal, regulatory requirements or expectations and recognised standards.<br>- Where available, online, real-time reporting tools are strongly encouraged. |
| Expertise, qualification and skills | - The auditing or certifying party and the person at the firm responsible for reviewing the certificate or report should have appropriate expertise, qualifications and skills. |
| Process | - Test the effectiveness of the service provider's key systems and controls.<br>- Be performed in line with recognised standards. |

8.9 In material outsourcing arrangements, the PRA expects firms to retain the contractual rights to:

- request an expansion of the frequency, number and type of certificates or reports supplied by the service provider, as well as their scope if justified from legal, regulatory or risk management perspectives; and

- perform onsite audits (individual or pooled) at their discretion.

### *Onsite audits*

8.10 Before an onsite audit, the PRA expects firms, individuals and organisations acting on their behalf to:

- provide reasonable notice to the service provider, unless this is not possible due to a crisis or emergency, or because it would defeat the purpose of the audit;

- verify that whoever is performing the audit has appropriate expertise, qualifications and skills; and

- take care if undertaking an audit of a multi-tenanted environment, eg a Cloud data centre, to avoid or mitigate risks to other clients of the service provider in the course of the audit (eg availability of data, confidentiality, impact on service levels).

### *Pooled audits*

8.11 Pooled audits may be organised by groups of firms sharing one or more service providers or facilitated by the service providers. They may be performed by representatives of the participating firms or specialists appointed on their behalf. Pooled audits can be more efficient and cost effective for firms and less disruptive for service providers running multi-tenanted environments. They can also help spread costs and disseminate best industry practices with regards to audit methods among firms.

8.12 Where pooled audits lead to common, shared findings, the PRA expects each participating firm to assess what these findings mean for it individually and whether they require any follow-up on their part.

# 9 Sub-outsourcing

9.1 The EBA Outsourcing Guidelines define 'sub-outsourcing' as 'a situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider', which may also include part of an outsourced function. Sub-outsourcing, which is also sometimes referred to as chain outsourcing, can amplify certain risks in material outsourcing, including:

- limiting firms' ability to manage the risks of the outsourcing arrangement. In particular, where there are large chains of sub-outsourced service providers spread across multiple jurisdictions; and
- giving rise to additional or increased dependencies on certain service providers, which the firm may be fully aware of or may not want.

9.2 An example of these dependencies may arise if:

- a firm enters into an outsourcing arrangement with a SaaS provider;
- the SaaS provider relies on Cloud infrastructure provided by a Cloud service provider; and
- the firm also has a direct, contractual relationship with the Cloud service provider, which means it relies on the same Cloud service provider both directly and indirectly.

## Firm oversight of sub-outsourcing

9.3 Where a material outsourcing arrangement is likely to involve sub-outsourcing, the PRA expects firms to assess relevant risks. Service providers can facilitate firms' due diligence by maintaining up to date lists of their sub-outsourced service providers.

9.4 The PRA expects firms to pay particular attention to the potential impact of large, complex sub-outsourcing chains on their operational resilience and ability to oversee outsourcing arrangements.

9.5 While it may not be feasible for firms to monitor every service provider across the supply chain, firms should, at a minimum, monitor those sub-outsourced service providers involved in the provision of important business services, including their ability to stay within the firm's impact tolerances.

9.6 Firms should only agree to sub-outsourcing if:

- the sub-outsourcing will not give rise to undue operational risk for the firm in line with Outsourcing 2.1(1) banks and Conditions Governing Business 7.2(2); and
- sub-outsourced service providers undertake to:
    - comply with all applicable laws, regulatory requirements and contractual obligations; and
    - grant the firm, Bank and PRA equivalent contractual access, audit and information rights to those granted by the service provider.

9.7 Firms should ensure that the service provider appropriately oversees sub-outsourced service providers, in line with their policy, as defined by the firm in Chapter 4. If the proposed sub-

outsourcing could have material adverse effects on a material outsourcing arrangement or would lead to a material increase of risk, the firm should exercise its right to object to the sub-outsourcing (if such a right was included in the agreement) and/or terminate the contract.

### Written agreement

9.8 In line with Chapter 6, the PRA expects written agreements for material outsourcing to indicate whether or not material sub-outsourcing is permitted, and if so:

- specify any activities that cannot be sub-outsourced;
- establish the conditions to be complied with in the case of permissible sub-outsourcing, including to:
    - specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the firm are continuously met.
- require the service provider to:
    - obtain prior specific or general written authorisation from the firm before transferring data (see Article 28 GDPR); and
    - inform the firm of any planned sub-outsourcing or material changes, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes to sub-contractors and to the notification period. Firms should be informed sufficiently early to allow them to at least carry out a risk assessment of the proposed changes and object to them before they come into effect.
- ensure that, where appropriate, firms have the right to:
    - explicitly approve or object to the intended sub-outsourcing or material changes thereto; and
    - ensure that the firm has the contractual right to terminate the agreement in the case of specific circumstances, eg where the sub-outsourcing materially increases the risks for the firm or where the service provider sub-outsources without notifying the firm.

# 10 Business continuity and exit plans

10.1 For each material outsourcing arrangement, the PRA expects firms to develop, maintain and test a:

- business continuity plan; and
- documented exit strategy, which should cover and differentiate between situations where a firm exits an outsourcing agreement:
    - in stressed circumstances, eg following the failure or insolvency of the service provider (stressed exit); and
    - through a planned and managed exit due to commercial, performance or strategic reasons (non-stressed exit).

10.2 The PRA's primary focus when it comes to business continuity plans and exit strategies is on the ability of firms to deliver important business services provided or supported by third parties in line with their impact tolerances in the event of disruption. Consequently, notwithstanding the importance of effectively planning for non-stressed exits, the main focus of this chapter is on business continuity and stressed exits.

## Business continuity

10.3 Firms should implement and require service providers in material outsourcing arrangements to implement appropriate business continuity plans to anticipate, withstand, respond to and recover from severe but plausible operational disruption.

10.4 An important objective of the access, audit and information rights in Chapter 8 is to enable firms, the PRA and Bank to assess the effectiveness of service providers' business continuity plans, in particular, the extent to which they may enable the delivery of important business services for which a firm relies (wholly or in part) on the service provider, within the firm's impact tolerance in severe but plausible scenarios.

10.5 In material Cloud outsourcing arrangements, the PRA 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, which may include:

- multiple data centres spread across geographical regions;
- multiple active data centres in different availability zones within the same region, which allows the service provider to re-route services if a data centre goes down;
- a hybrid Cloud (ie a combination of on-premise and public Cloud data centres)
- multiple or back-up vendors;
- retaining the ability to bring data or applications back on-premise; and/or
- any other viable approach that can achieve and promote an appropriate level of resiliency.

10.6 The PRA expects firms to consider the implications of deliberately destructive cyber-attacks when establishing or reviewing data recovery capabilities, either individually or collaboratively.

10.7 In line with FR 7, In the event of a disruption or emergency (including at an outsourced or third party service provider), firms should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the Bank, PRA, FCA and, if relevant, the service providers themselves are informed in a timely and appropriate manner.

### Stressed exits

10.8 Firms' exit plans should cover stressed exits and be appropriately documented and tested as far as possible.

10.9 A key objective of the stressed exit part of exit plans is to provide a last resort risk mitigation strategy in the event of disruption that cannot be managed through other business continuity measures, including those mentioned in the previous section, eg the insolvency or liquidation of a service provider.[47]

10.10 The PRA does not prescribe or have a preferred form of exit in stressed scenarios. Its focus is on the outcome of said exit, ie the continued provision by the firm of important business services provided or supported by third parties, rather than the method by which it is achieved.

10.11 The PRA does, however, expect firms to consider all potentially viable forms of exit in a stressed exit scenario, which may include:

- bringing the data, function or service back in-house/on-premise;
- transferring the data, function or service to an alternative or back-up service provider; or
- any other viable methods.

10.12 The PRA expects firms to give meaningful consideration to all available tools that can facilitate an orderly stressed exit from a material outsourcing arrangement. These tools are constantly evolving, in particular in technology outsourcing, including Cloud, and may include:

- new potential service providers;
- technology solutions and tools to facilitate the switching and portability of data and applications; and
- industry codes and standards.

10.13 Firms should also actively consider temporary measures that can help ensure the ongoing provision of important business services following a disruption and/or a stressed exit, even if these are not suitable long-term solutions, eg contractual arrangements allowing for continued use of a service or technology for a transitional period following termination.

47 In intra-group outsourcing scenarios, the stressed parts of these exit plans can also help facilitate compliance with Operational Continuity 4.4 where applicable.

## Governance of business continuity plans and exit plans

10.14 Firms should develop their business continuity and exit plans, in particular for stressed exits, during the pre-outsourcing phase once they have determined that a planned outsourcing arrangement is material (see Chapter 5). Doing so will enable them to:

- use the due diligence process to identify potential alternative or back-up service providers;
- estimate the cost, resourcing and timing implications of the proposed business continuity or exit plan in both stressed and non-stressed scenarios as part of the risk assessment;
- identify data they may need to access, recover or transfer as a priority in a disruption or stressed exit; and
- define the key KPIs and key risk indicators (KRIs) which, if breached, may trigger an exit (both stressed and non-stressed).

10.15 Firms should assign clear roles and responsibilities for business continuity and exit plans. Subject to proportionality, they may establish cross-disciplinary teams to develop, document, test and execute their business continuity and exit plans, especially in stressed scenarios (which may include communicating with the PRA and other relevant stakeholders in the event of disruption). Based on the size and complexity of the firm, these teams may include relevant business lines, control functions, technical experts (eg IT specialists) and be chaired by an SMF. Firms should also allocate responsibility for signing off business continuity and exit plans, including updates thereafter, and the decision to activate them.

10.16 When developing business continuity and exit plans, firms should define the objectives of the plan, including what would constitute successful business continuity or a successful exit in both stressed and non-stressed scenarios, by reference to measurable criteria such as costs, functionality, time and the firm's impact tolerances for important business services.

10.17 Firms should take reasonable steps to test exit plans; in particular, those relating to stressed exits. The extent and nature of testing will vary depending on the type of outsourcing arrangement and corresponding exit plan. For instance, a firm running a hybrid Cloud structure may take into account the potential back-up functions located in its private Cloud elements. Likewise, a firm that keeps backup copies of data which it has outsourced to the Cloud outside the Cloud environment may focus its testing on assessing the ongoing consistency of both sets of data and reconciling them as appropriate. Firms should also assess and take reasonable steps to manage any operational risks which may be caused or increased by the actual testing (eg data theft).

10.18 Business continuity and exit plans should be reviewed periodically to take into account developments that may change the feasibility of the business continuity measures or an exit, eg:

- an increase in the number of availability zones or regions offered by a current service provider;
- changes to the firm's business requirements;
- the emergence of new, potentially viable alternative providers; and/or
- developments in technology or other tools to facilitate the porting of data and applications, eg among Cloud providers or between firms' on-premise environments and the Cloud.

**TABLE 9: Contingency Planning in outsourced insurance policy administration**

| **Contingency Planning – Observed best practice in insurers** |
| --- |
| A 2019 PRA supervision conducted a thematic review of insurers' contingency plans in the event of the failure of a material outsourced service provider providing policy administration services. They identified the following good practices, which insurers may wish to consider when conducting their contingency planning:<br><br>• Proposals to act collaboratively with other insurers who share a common outsourcer, in the event of outsourcer failure.<br><br>• Evidence of awareness of the challenges of utilising step-in rights where there are shared services.<br><br>• Evidence that the contingency plans had been signed off at an appropriately senior level given the criticality of the outsourced service.<br><br>• A list of named contacts and details documented of individuals and teams responsible for implementing the contingency plan.<br><br>• Evidence that contractual provisions took contingency planning into consideration. For instance, by including provisions on:<br><br>  ○ step-in rights;<br><br>  ○ provisions to transfer employees of the service provider to the insurer under the Transfer of Undertakings (Protection of Employment) Regulations (TUPE); and<br><br>  ○ access by the insurer to necessary data and systems of the service provider.<br><br>• Consideration of a range of scenarios in which a contingency plan may need to be used, including:<br><br>  ○ financial and/or operational failure of the service provider; and<br><br>  ○ if the service provider enters or is at risk of entering into administration or liquidation.<br><br>• An assessment of the:<br><br>  ○ substitutability of the service being outsourced;<br><br>  ○ availability of alternative service providers;<br><br>  ○ cost and resource implications of implementing a given contingency plan. For example, if an insurer intends to bring an outsourced service back in-house as part of its contingency plan it should consider whether it would require more staff, where these staff would be based and whether the necessary infrastructure is in place to support its continued delivery of the service; and<br><br>  ○ time it would take to implement a given contingency plan.<br><br>• Evidence that key assumptions made in the assessments have been tested. |

# Appendix: Guidance for completing the Outsourcing Register

| | EBA Outsourcing Guidelines paragraph | Common Issues | Guidance for Firms |
|---|---|---|---|
| **All Outsourcing Agreements** | Para 54(a)<br>A reference number for each outsourcing arrangement. | Firms may use different reference numbers. | |
| | Para 54(b)<br>- the start date and, as applicable,<br>- the next contract renewal date,<br>- the end date<br>- and/or notice periods for the service provider and for the institution. | | Report dates in a YYYYMMDD format |
| | Para 54(c)<br>A brief description of the outsourced function, including the data that are outsourced and<br><br>whether or not personal data (eg by providing a yes or no in a separate data field) have been transferred or if their processing is outsourced to a service provider. | Free text can be difficult to analyse and compare. | Firms to describe the function in 250 characters. |
| | Para 54(d)<br>A category assigned by the institution that reflects the nature of the function as described above (eg information technology (IT), control function), which should facilitate the identification of different types of arrangements. | Firms may use inconsistent categories to describe the nature/type of outsourcing arrangement. | |
| | Para 54(e)<br>- the name of the service provider<br>- the corporate registration number<br>- the legal entity identifier (where available)<br>- the registered address<br>- other relevant contact details, and<br>- the name of its parent company (if any). | Firms may name the same service provider in different ways eg using initials or full names. | Use a standard legal entity identifier.<br><br>Possibilities include:<br>LEI,<br>GEMS ID. |
| | Para 54(f)<br>The country or countries where the service is to be performed, including the location (ie country or region) of the data. | | |
| | Para 54(g)<br>- Is the outsourced function 'critical' or 'important'?<br>- and a brief summary of the reasons why it's considered critical or important. | Free text can be difficult to analyse and compare. | Firms to describe why agreement is deemed material in 250 characters. |

| | | | |
|---|---|---|---|
| | Para 54(h)<br>- in the case of outsourcing to a cloud service provider, the cloud service and deployment models, ie public/private/hybrid/community,<br>- the specific nature of the data to be held<br>- and the locations (ie countries or regions) where such data will be stored. | Different institutions may define the 'specific nature of the data to be held', differently, making it difficult to analyse and compare. | Firms to summarise the specific nature of the data being held in 250 characters. |
| | Para 54(i)<br>the date of the most recent assessment of the criticality or importance of the outsourced function. | Firms may undertake multiple assessments, within a period of time. | Report dates in a YYYYMMDD format |
| | | | |
| **Material Outsourcing Arrangements** | Para 55(a)<br>the institutions, payment institutions and other firms within the scope of the prudential consolidation or institutional protection scheme, where applicable, that make use of the outsourcing. | Firms may use different names for various group legal entities | Link to firm's FRN / other identifier if based outside the UK |
| | Para 55(b)<br>whether or not the service provider or sub-service provider is part of the group or a member of the institutional protection scheme or is owned by institutions or payment institutions within the group or is owned by members of an institutional protection scheme. | | |
| | Para 55(c)<br>the date of the most recent risk assessment and a brief summary of the main results. | Free text can be difficult to analyse and compare. | Report dates in a YYYYMMDD format. Firms to summarise risk assessment in 250 characters. |
| | Para 55(d)<br>the individual or decision-making body (eg the management body) in the institution that approved the outsourcing arrangement. | There could be more than one SMF that approved the outsourcing arrangement. | |

| | | | |
|---|---|---|---|
| | Para 55(e)<br>the governing law of the outsourcing agreement. | | |
| | Para 55(f)<br>the dates of the most recent and next scheduled audits, where applicable. | | Report dates in a YYYYMMDD format. |
| | Para 55(g)<br>- the names of any sub-contractors to which material parts of a critical or important function are sub-outsourced, including:<br><br>- the country where the sub-contractors are registered,<br>- where the service will be performed, and<br>- the location (ie country or region) where the data will be stored. | Firms may name the same service provider in different ways eg using initials or full names.<br><br>- Countries could be describe differently. | Use a standard legal entity identifier.<br><br>Possibilities include:<br>LEI,<br>GEMS ID. |
| | Para 55(h)<br>- the outcome of the assessment of the service provider's substitutability (eg easy, difficult or impossible).<br><br>- the possibility of reintegrating a critical or important function into the institution<br><br>OR<br><br>- the impact of discontinuing the critical or important function. | 'Easy', 'Difficult', and 'Impossible' = difficult to quantify as it's subjective.<br><br>Free text responses could be difficult to analyse between the different institutions. | Firms to summarise in 250 characters why 'difficult' or 'impossible' if chosen.<br><br>Firms to describe in 250 characters the impact of discontinuing the function. |
| | Para 55(i)<br>identification of alternative service providers in line with the point above. | Firms may name the same service provider in different ways eg using initials or full names. | |
| | Para 55(j)<br>whether the outsourced 'critical or important function' supports business operations that are time-critical. | 'Time-critical' needs defining. | Tie the definition of 'Time Critical' to impact tolerances? |
| | Para 55(k)<br>the estimated annual budget cost. | | |