This SS comes into effect on Thursday 31 March 2022. For more information, please see:
https://www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Publication

Supervisory Statement | SS2/21

Outsourcing and third party risk management

March 2021

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Supervisory Statement | SS2/21

Outsourcing and third party risk management

March 2021

Prudential Regulation Authority | 20 Moorgate | London EC2R 6DA

Contents

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 the scope of existing requirements on outsourcing and some of the detailed expectations in this SS. However, these third party arrangements are still subject to the PRA Fundamental Rules and other PRA requirements and expectations on business continuity, governance, operational resilience, and risk management (including but not limited to cyber risk).

- Chapter 3 clarifies how the principle of proportionality applies to the expectations in this SS. In particular, to intragroup 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.

- Chapter 5 sets out the PRA's expectations for firms during the pre-outsourcing phase. It addresses the materiality and risk assessments of their outsourcing and other third party arrangements (including notification to the PRA where required), and firms' due diligence on third parties.

- Chapter 6 lists the areas that 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:

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

1.5 The aims of this SS are to:

- '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;

- complement the requirements and expectations on operational resilience in the PRA Rulebook; SS1/21 'Operational resilience: Impact tolerances for important business services'; and the Statement of Policy (SoP) 'Operational resilience'; and[1]

- implement the:

  - European Banking Authority (EBA) 'Guidelines on outsourcing arrangements' (EBA Outsourcing GL).[2] This SS clarifies how the PRA expects banks to approach the EBA Outsourcing GL in the context of its requirements and expectations. In addition, certain chapters in this SS expand on the expectations in the EBA Outsourcing GL, for instance Chapters 7 (Data security) and 10 (Business continuity and exit plans); and[3]

  - relevant sections of the EBA 'Guidelines on ICT and security risk management' (EBA ICT GL).[4]

1.6 In line with the Statement of Policy (SoP) 'Interpretation of EU Guidelines and Recommendations: Bank of England and PRA approach after the UK's withdrawal from the EU',[5] the PRA has not formally implemented the following Guidelines, which came into force after the implementation period:

- European Insurance and Occupational Pensions Authority (EIOPA) 'Guidelines on outsourcing to cloud service providers' (EIOPA Cloud GL);[6]

- EIOPA 'Guidelines on information and communication technology security and governance' (EIOPA ICT GL);[7]

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

2 The PRA website hosts the Guidelines and Recommendations that were complied with in the UK before the end of the transition period. The EBA Outsourcing GL are available at: https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/december/gl-outsourcing-arrangements.pdf.

3 The terms contingency and continuity plan stem from European legislation. They are used interchangeably in this SS.

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

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

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

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

- European Securities and Markets Authority (ESMA) 'Guidelines on outsourcing to cloud service providers' (ESMA Cloud GL);[8]

1.7 However, the PRA took these draft Guidelines into consideration when developing its policy and considers that the expectations in this SS are at least equivalent to them in effectiveness and substance. The PRA sought to avoid undue divergences from the draft Guidelines referred to in paragraph 1.5, but it followed its own approach where it deemed it to be beneficial, or to advance the PRA's statutory objectives. In particular, this SS complements and strengthens the PRA's requirements and expectations on operational resilience and aims promotes consistency among banks and insurers. The SS should be the primary source of reference for UK firms when interpreting and complying with PRA requirements on outsourcing and third party risk management. Firms with operations in both the UK and the EU should comply with applicable Guidelines in respect of their EU operations.

1.8 To ensure a consistent approach across PRA-regulated firms, the expectations in this SS apply to all forms of outsourcing and, where indicated, other non-outsourcing third party arrangements entered into by firms. In addition, this SS includes specific examples, references, and 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'.[9] In developing the expectations in this SS, including in relation to cloud usage, the PRA has taken into account international standards including but not limited to the:

- Basel Committee on Banking Supervision (BCBS) [draft] 'Principles for operational resilience' (BCBS Operational Resilience Principles);[10]

- Financial Stability Board (FSB) 'Effective Practices for Cyber Incident Response and Recovery' (FSB Effective Practices);[11]

- 'G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector' (G-7 Third-Party Elements);[12] and

- International Organisation of Securities Commissions' (IOSCO) [draft] 'Principles on Outsourcing'.[13]

1.9 To promote clarity and certainty, this SS references other regulatory requirements that govern outsourcing (and in some cases other third party arrangements) 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 below.

Table 1: Existing requirements and expectations on outsourcing for banks and insurers[14]

Banks	Insurers
Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing MiFID II as it forms part of retained EU law (MODR), Articles 30–32	Commission Delegated Regulation (EU) 2015/35 supplementing Solvency II as it forms part of retained EU law (Solvency II Delegated Regulation), Articles 274 and 294(8)

8 https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf.
9 https://www.bankofengland.co.uk/research/future-finance.
10 https://www.bis.org/bcbs/publ/d509.pdf.
11 https://www.fsb.org/wp-content/uploads/P191020-1.pdf.
12 https://www.fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf.
13 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf.
14 Unless otherwise stated, any references to EU or EU derived legislation refer to the version of that legislation which forms part of the body of EU law which was retained in the UK.

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	Rules 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 Insurance – Operational Resilience Part of the PRA Rulebook
Rules 2.5 and 4.1 of the Operational Resilience Part of the PRA Rulebook	EIOPA Guidelines on the System of Governance,[15] Guidelines 14 and 60–64
Rules 10.1 and 10.2 of the Internal Capital Adequacy Assessment Part of the PRA Rulebook	
EBA Outsourcing Guidelines	SS35/15 'Strengthening individual accountability in insurance',[16] paragraphs 2.22A, 2.22L, 2.31, 2.33, 2.37A, 2.37B, 2.40, 2.52, and 2.93
EBA 'Guidelines on information and communications technology (ICT) and security risk management'	
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 GL)	
EBA 'Recommendations on outsourcing to cloud service providers' (EBA Cloud Recommendations) until superseded by the EBA Outsourcing GL	
SS28/15 'Strengthening individual accountability in banking',[17] paragraphs 2.11G, 2.41A	
SS21/15 'Internal governance',[18] paragraphs 2.15, 2.23	
SS9/16 'Ensuring operational continuity in resolution,'[19] paragraphs 2.1, 5.1, 5.10, 6.1, 8.2, 11.5, and Chapter 4.	
PRA Statement of Policy (SoP) on Operational Resilience	
SS29/19 'Operational resilience: Impact tolerances for important business services'	

1.10 The PRA considers that the expectations in the SS are compatible 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 are set out mainly in the Systems and Controls (SYSC) Sourcebook of the FCA Handbook[20] (in particular SYSC8 (banks) and SYSC13.9 (insurers)), as well as in FCA 'Finalised Guidance 16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services', where applicable.[21]

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

1.11 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

15 https://eiopaeuropa.eu/guidelinessii/eiopa_guidelines_on_system_of_governance_en.pdf.
16 July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-insurance-ss.
17 July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss.
18 April 2017: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/internal-governance-ss.
19 July 2016: https://www.bankofengland.co.uk/prudential-regulation/publication/2016/ensuring-operational-continuity-in-resolution-ss.
20 https://www.handbook.fca.org.uk/handbook/SYSC/.
21 https://www.fca.org.uk/publications/finalised-guidance/fg16-5-guidance-firms-outsourcing-cloud-and-other-third-party-it.

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
Information Gathering 2.2 and 3.3	Chapter 2 of the Non-Solvency II Firms – General Powers Part of the PRA Rulebook
Notifications 2.3(1)(e)	Information Gathering 2.2 and 3.3
Allocation of Responsibilities 5.2 (3),(4), and (6)	Notifications 2.3(1)(e)
	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)

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 (Commission Delegated Regulation on organisational requirements and operating conditions) and Article 13(28) of Solvency II. In line with the EBA Outsourcing GL, when considering whether an arrangement with a third party falls within the definition of outsourcing, firms should consider whether the third party will perform the relevant function or service (or part thereof) on a recurrent or an ongoing basis.

2.2 Existing requirements on outsourcing, including 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 the definition of outsourcing. In line with the definition in the G7 Third Party Elements and EBA ICT GL, 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'.

Expectations for non-outsourcing third party arrangements

2.3 The PRA's overarching aim is for firms to apply adequate governance and controls to all third party dependencies that can impact its statutory objectives. Examples include those that support the provision of important business services or carry a high level of risk. The [draft] BCBS Operational Resilience Principles refer to this principle as 'third party dependency management'.

2.4 The EBA Outsourcing GL provide examples of arrangements between banks and third parties which 'as a general principle [banks] should not consider as outsourcing' (hereafter referred to as 'non-outsourcing third party arrangements') (see paragraph 28 of the EBA Outsourcing GL). Non-outsourcing third party arrangements are not covered by the granular requirements applicable to outsourcing arrangements referred to in paragraph 2.2. Other examples of non-outsourcing third party arrangements may include but are not limited to:

- purchases of hardware, software, and other ICT products, such as:

(a) the design and build of an on-premise IT platform;

(b) the purchase of data collated by third party providers (data brokers), eg geospatial data or data from in-app device activity, social media, etc.; and

(c) 'off-the shelf' machine learning models, including samples of the data used to train and test the models, open source software, and machine learning libraries developed by third party providers; and

- in the case of insurers, the use of aggregators, such as pricing comparison platforms, and delegated underwriting.

2.5 As some non-outsourcing third party arrangements may also impact the PRA's objectives, the PRA expects firms to assess the materiality and risks of all third party arrangements irrespective of whether they fall within the definition of outsourcing. Firms should use all relevant criteria in Chapter 5 in their assessments (however, some criteria may be inapplicable to certain non-outsourcing third party arrangements).

2.6 Where a firm deems a non-outsourcing third party arrangement 'material' or 'high risk', it should implement proportionate, risk-based, suitable controls. These controls do not necessarily have to be the same as those that apply to outsourcing arrangements. However, the controls should be appropriate to the materiality and risks of the third party arrangement and as robust as the controls that would apply to outsourcing arrangements with an equivalent level of materiality or risk. It follows that firms should apply stricter controls to material, non-outsourcing third party arrangements than to non-material outsourcing arrangements.

2.7 The PRA reminds firms that the following requirements apply to all third party arrangements irrespective of whether or not they fall under the definition of 'outsourcing':

- PRA Fundamental Rules 2, 3, 5 and 6, and 7;

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

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

- Rule 10 in the Internal Capital Adequacy Assessment Part of the PRA Rulebook (banks);

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

- all relevant requirements in the Operational Resilience and Insurance – Operational Resilience Parts of the PRA Rulebook.

2.8 In line with the expectations in Chapter 4 of this SS, firms may implement a holistic, single third party risk management policy covering outsourcing and non-outsourcing third party arrangements. Alternatively, they may have separate policies on each of those respective areas provided that they are aligned, consistent, effective, and suitably risk-based.

Third party ICT arrangements

2.9 The following standards apply to all third party ICT arrangements:

- EBA ICT GL, including but not limited to Sections 3.2.3, 3.3.2, 3.4.5, and 3.7 (in particular, paragraph 86). These GL should be interpreted consistently with: the Operational Resilience/Insurance – Operational Resilience Parts, the expectations in this SS, and SS1/21; and

- relevant legal requirements and standards on ICT security (eg Cyber Essentials Plus) and data protection, including but not necessarily limited to General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2.10 The PRA also encourages firms to take into account global standards on ICT risk management, including but not necessarily limited to the toolkit in the FSB Effective Practices (in particular, paragraphs 13, 18, 19 and 20, 33 and 36), and the G7 Third party Elements.

Third party arrangements subject to regulatory requirements

2.11 Certain arrangements among regulated financial institutions, including between firms that are not part of the same group and between firms and financial market infrastructures, do not fall within the definition of outsourcing in paragraph 2.1. These arrangements include clearing, settlement, custody services, and certain services provided by Lloyd's of London, all of which are subject to specific regulatory requirements. For instance, custody services are regulated by the Client Assets Sourcebook in the FCA Handbook and Central Securities Depositories Regulation. They are also subject to the requirements in paragraph 2.7 of this SS.[22]

2.12 While these arrangements do not fall under the definition of outsourcing, they are third party arrangements that can give rise to significant risks to the PRA's objectives and should be subject to appropriate monitoring and risk-based controls. The PRA therefore expects firms that are parties to these arrangements, either as service providers or service recipients, to leverage applicable, existing regulatory requirements to manage relevant risks and promote an appropriate level of resilience.

3 Proportionality

3.1 Firms should meet the expectations in this SS in a manner appropriate to: their size and internal organisation; the nature, scope, and complexity of their activities; and the criticality or importance of the outsourced function, 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, including its systemic significance. 'Materiality' assesses the potential impact of a given outsourcing or third party arrangement on a firm's safety and soundness, including: its operational resilience; its ability to comply with legal and regulatory obligations; the risk that firms' ability to meet these obligations could be compromised if the arrangement is not subject to appropriate controls and oversight; 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 as appropriate.

22 https://www.handbook.fca.org.uk/handbook/CASS.pdf.

Intragroup outsourcing

3.3 Intragroup 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 intragroup outsourcing 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) of the Solvency II Delegated Regulation, firms may comply with some of these requirements proportionately depending on their level of 'control and influence' over the entity that is providing the outsourced service.

3.5 Control and influence may vary depending on the characteristics of a group. For instance, a firm that outsources to a subsidiary may have greater control and influence than one that outsources to its parent company. The following factors may also be relevant when determining the level of control and influence:

- the group's governance structure, including the level of connectivity between the firm's and group's boards, board committees, executive committees, internal control functions and/or other relevant functions (eg technology);

- the allocation of senior management functions (SMFs) and responsibilities throughout the group;

- the ability of a firm to alter its intragroup outsourcing arrangements and/or influence their terms and conditions to ensure they meet its UK regulatory obligations and manage relevant firm and UK-specific risks; and

- the consistency and robustness of group wide standards controls, policies, and procedures, (eg on business continuity).

3.6 Depending on its level of control and influence in respect of intragroup outsourcing arrangements, a firm may, for example:

- adjust its vendor due diligence, although firms should still carefully assess whether a potential service provider that is part of its group has the ability, capacity, resources, and appropriate organisational structure to support the performance of the outsourced function or third party service;

- if a UK consolidated group is entering into a material outsourcing arrangement that covers the entire group or multiple firms in it, a single notification may be enough to meet its obligations under Rule 2.31(e) in the Notifications Part of the PRA Rulebook, provided that it lists all the individual firms that will receive the relevant material outsourcing service;

- rely on the group's potentially stronger negotiating and purchasing power to enter into group-wide arrangements with external third parties;

- adapt certain clauses in outsourcing agreements (a written agreement is always required – even in intragroup arrangements; see Chapter 6);

- 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, such as binding corporate rules for international data transfers);

- rely on a centralised group process for overseeing external third party service providers, including the exercise of access, audit, and information rights, provided that this process appropriately takes into account and documents any legal entity-specific risks and allows for legal entity-specific risk mitigation where necessary; and

- rely on business continuity, contingency, and exit plans developed at group level, provided that they adequately safeguard their operational resilience.

Leveraging existing regulatory frameworks

3.7 Where relevant, firms may be able to leverage compliance with existing requirements in other areas of regulation to help meet their regulatory obligations in respect of their intragroup outsourcing arrangements. For instance, for some banks, intragroup outsourcing arrangements may be subject to the requirements in Operational Continuity Chapter 4 and Chapters 9 and 12 in the Ring-Fenced Bodies Part of the PRA Rulebook. Compliance with these requirements may also mean those banks meet certain expectations in this SS in respect of intragroup outsourcing arrangements (for instance, in respect of business continuity and exit plans (see Chapter 10)). The PRA also expects firms to consider whether they can leverage elements of their operational continuity in resolution (OCIR) record-keeping to identify and document their intragroup dependencies, as long as relevant information is clear and readily available to the PRA upon request.[23]

3.8 Firms may also leverage their end-to-end mapping of important business services under Chapter 4 of the Operational Resilience – CRR Firms and Operational Resilience – Solvency II Parts of the PRA Rulebook to document and map their intragroup and other dependencies.

Non-significant firms

3.9 The PRA Rulebook does not define a 'significant' firm and it is for firms to determine their own significance. For the purposes of this SS, firms with a supervisory contact who has indicated they are impact category 1 or 2 should consider themselves 'significant'. This approach is consistent with the definitions of 'significant firm' in:

- 'The PRA's approach to banking supervision' and 'The PRA's approach to insurance supervision' ('PRA Approach Documents');[24]

- the EBA Outsourcing GL and EBA Governance GL;[25] and

- for Solvency II insurers, SS10/16 'Solvency II: Remuneration requirements'.[26]

3.10 'Non-significant' firms may meet certain expectations in this SS in a proportionate manner. The PRA's supervisory scrutiny of firms' outsourcing arrangements may also reflect their significance.

Governance and internal controls

3.11 The PRA recognises that new and growing firms frequently tend to rely more extensively on outsourcing and third party products and services given the benefits they can bring in terms of lower

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 CRDV (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.

barriers to entry, cost savings, and in some cases increased operational resilience.[27] However, to meet the Threshold Conditions on an ongoing basis, all firms must retain appropriate non-financial resources, including to effectively oversee these outsourced and third party services (see Chapter 4).

3.12 An example of a function that 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. Likewise, although non-significant firms' outsourcing policies should include the minimum requirements outlined 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

3.14 Although all firms are in principle able to use the access, audit, and information-gathering tools highlighted in Chapter 7, including third party certification and pooled audits, these tools may be particularly useful for non-significant firms as a means of mitigating 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.

Third-country branches

3.15 Outsourcing arrangements by UK branches of third-country firms (third-country branches) are subject to the requirements in Chapter 7 of the Internal Governance of Third Country Branches Part of the PRA Rulebook (banks) and Conditions Governing Business Chapter 7 (insurers).

3.16 Since Friday 1 January 2021, the parts of the PRA Rulebook referred to in paragraph 3.15 apply to UK branches of European Economic Area (EEA) firms that were previously operating in the UK under passporting.

3.17 While the PRA's application of outsourcing requirements and expectations on third-country branches diverges from the approach set out in the EBA Outsourcing GL, which do not treat the provision of services by EU firms to their branches in the EEA as 'outsourcing', it is justified by the:

- importance of effective risk management and controls in all third-country branches deemed to be systemic due to their potential impact on financial stability in the UK; and
- need to treat all third-country branches consistently.

3.18 At a minimum, the PRA expects third-country branches to have:

- a clear, documented list of their intragroup outsourcing arrangements, which should identify those deemed material;

[27] See CP9/20, July 2020: https://www.bankofengland.co.uk/prudential-regulation/publication/2020/new-and-growing-banks.

- documented written agreements, such as service level agreements, for all intragroup outsourcing arrangements (in particular those deemed material), setting out expected service levels and key performance indicators (KPIs);

- appropriate monitoring and oversight of their intragroup outsourcing arrangements, including appropriate visibility of the whole firm's or parent's material sub-outsourced service providers and supply chain by internal control functions and, if applicable, other areas such as technology;

- effective processes and mechanisms for escalating concerns, issues, and regulatory feedback relating to their intragroup outsourcing arrangements to the whole firm or group.

3.19 The PRA recognises the need to apply the expectations in this SS proportionately to third-country branches. In addition to the guidance on intragroup arrangements in paragraph 3.5, third-country branches can rely on:

- due diligence, materiality assessments, and risk assessments of third-parties outside their group undertaken by and on behalf of the whole firm provided that they take into account their UK regulatory obligations (see Chapter 5);

- contractual arrangements between third parties outside their group and the whole firm or group (see Chapter 6);

- audits of external third party service providers performed by or on behalf of the whole firm or group as long as they provide them with appropriate assurance and information to comply with their UK regulatory obligations; and/or

- firm or group-wide business continuity plans and exit strategies. Systemic wholesale branches should, however, take reasonable steps to develop local business continuity, contingency planning, and exit strategies (if available) covering any activities or services which they provide that could impact UK financial stability.

4 Governance and record-keeping

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

- board engagement on outsourcing;

- allocation of responsibilities;

- outsourcing and the 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 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 and non-outsourcing third party arrangements, 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' and third party risk management;
- 'bear responsibility for the effective management of all risks to which the firm is exposed', including by:
  - appropriately 'identifying and [having an] 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'.[28]

In line with SS5/16 'Corporate governance: Board responsibilities', the PRA expects management information on outsourcing provided to the board to be clear, consistent, robust, timely, and well-targeted, and to contain an appropriate level of technical detail to facilitate effective oversight and challenge by the board.[29]

Shared responsibility model

4.5 As part of ensuring effective governance of an outsourcing arrangement, the PRA expects firms to define, document, and understand their and the service provider's respective responsibilities. In the case of cloud computing, the term commonly used to help firms and cloud providers understand their respective obligations is the 'shared responsibility model'.

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

28 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.

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

Table 3: The shared responsibility model in cloud outsourcing

Cloud service providers tend to operate under the 'shared responsibility model' whereby:

- the firm is responsible for what's in the cloud and the cloud service provider is responsible for the provision of the cloud;
- firms remain responsible for correctly identifying and classifying data in line with their legal and regulatory obligations, and adopting a risk based approach to the location of data. They also remain responsible for configuration and monitoring of their data in the cloud to reduce security and compliance incidents;
- Cloud service providers assume responsibility for the infrastructure running the outsourced service, eg data centres, hardware, software etc.; and
- 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.[30]

Empty shells

4.6 Firms should avoid becoming 'empty shells' that are incapable of meeting the Threshold Conditions. The following Threshold Conditions are particularly relevant:

- being capable of being effectively supervised by the PRA;
- the 'suitability' Threshold Condition in Sections 4E (Part 1A) (insurers) and 5E (Part 1E) (banks) of FSMA. 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. Further guidance on the PRA's approach to the Threshold Conditions is set out in paragraph 21 of 'The PRA's approach to banking supervision' and paragraph 25 of 'The PRA's approach to insurance supervision' (together, the 'Approach Documents').[31]

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 The PRA generally expects but does not require this Prescribed Responsibility to be allocated to (one of) the individuals performing the Chief Operations Senior Management Function (SMF24) if a firm has one or more individuals performing that SMF. As noted in SS28/15 for banks and SS35/15 for insurers, the SMF24 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 or other areas of the firm. 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.

30 As defined in the EBA Outsourcing Guidelines.
31 https://www.bankofengland.co.uk/prudential-regulation/publication/pras-approach-to-supervision-of-the-banking-and-insurance-sectors.

Outsourcing policy

4.10 Firms' boards should approve, regularly review, and implement a written outsourcing policy. As noted in Chapter 2 of this SS, firms may 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;
- ICT;
- information and cyber 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, including those on outsourcing, ICT, information security, or operational resilience. Where firms' policies include confidential or sensitive information, firms can omit or redact it and only share those sections relevant to the performance of the outsourced or third party service. Sharing these policies with third party service providers does not dilute firms' responsibilities in terms of managing their outsourcing and third party arrangements, but can help third party service providers get a better understanding of firms' regulatory obligations and other relevant aspects such as their risk tolerance and expected service levels.

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, and the policy does not have to be contained in a single document. 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 4.

Table 4: Contents of the outsourcing policy

General	• The responsibilities of the board, including its involvement, as appropriate, in decisions about material outsourcing. • The involvement of business lines, internal control functions, and other individuals (in particular, SMFs) in respect of outsourcing arrangements.[32] • Links to other relevant policies (see paragraph 4.8). • Documentation and record-keeping. • Procedures for the identification, assessment, management, and mitigation of potential relevant conflicts of interest.[33] • Business continuity planning (BCP) (see paragraph 4.10). • Differences, if any, between the approach to: - intragroup outsourcing vs outsourcing to external service providers; - material vs non-material outsourcing; - outsourcing to service providers regulated or overseen by the Bank, PRA, or FCA vs unregulated service providers; and - 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). • 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: - day-to-day oversight, including incident reporting, periodic performance assessment against service level agreements, and periodic strategic assessments; - being notified and responding to changes to an outsourcing arrangement or service provider (eg to its financial position, organisational or ownership structures, or sub-outsourcing); - independent review and audit of compliance with legal and regulatory requirements and policies; and - renewal processes.
Termination	Exit strategies and termination processes, including a requirement for a documented exit plan for material outsourcing arrangements where such an exit is considered possible, explicitly catering for the unexpected termination of an outsourcing agreement (a stressed or unplanned exit), and taking into account possible service interruptions (and the firm's impact tolerance for important business services)(see Chapter 10).

Record-keeping

4.15 The PRA expects all firms to keep appropriate records of their outsourcing arrangements. The PRA considers that a firm, in complying with 2.3(1)(e) of the Notifications Part of the PRA Rulebook, would likely already have records of its material outsourcing arrangements for this purpose. The records should also be sufficient to enable the firm to fulfil the expectations concerning concentration risk set out in 5.24. Firms should also make any information on their outsourcing and

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

third party arrangements of which the PRA would reasonably expect notice available to it in accordance with Fundamental Rule 7. The PRA may, if appropriate and justified, also request data on firms' outsourcing arrangements under section 165 of FSMA.[34]

4.16 From Friday 31 December 2021, the EBA Outsourcing GL 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'). 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 on Friday 31 December 2021.

5 Pre-outsourcing phase

5.1 The PRA expects firms to:

- determine the materiality of every outsourcing and third party 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'.[35]

5.3 Materiality should be read as incorporating the concept of a 'critical or important operational function' in relevant retained EU legislation. The requirements in Article 31 of MODR or Article 274(5) of the Solvency II Delegated Regulation 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 help firms avoid confusion with different but partly overlapping terms that exist in financial regulation, such as 'critical function' or 'critical service' in an OCIR context. For all intents and purposes, the PRA considers that a 'material outsourcing' arrangement encompasses a 'critical or important outsourcing' arrangement in relevant retained EU legislation. Moreover, the criteria that firms should take into account when identifying 'material outsourcing' arrangements is substantively aligned to the criteria for identifying 'critical or important outsourcing arrangements' under the EBA Outsourcing GL with a few justified exceptions, such as those that reference the PRA's requirements on operational resilience (see paragraphs 5.11–5.13 below).

5.5 If a firm outsources services to which OCIR applies, this arrangement will generally constitute 'material outsourcing'. However, outsourcing and non-outsourcing third party arrangements that are

34 The PRA may exercise, under section 165A of the Financial Services and Markets Act 2000 (FSMA), the power to require certain persons to provide (i) specified information or information of a specified description; or (ii) specified documents or documents of a specified description, that it considers are, or might be, relevant to the stability of one or more aspects of the UK financial system (the financial stability information power).

35 See the Notifications 2.3(e) Part of the PRA Rulebook.

not within scope of OCIR might still be 'material outsourcing' if they could affect the PRA's objectives outside of an OCIR context. Examples may include outsourcing arrangements involving personal or sensitive data or carrying high reputational risk.

5.6 Although the term 'material outsourcing' in the PRA Rulebook is limited to outsourcing arrangements, the concept of materiality itself and the criteria in this chapter apply to all third party arrangements. Firms should determine the materiality of all third party arrangements using all relevant criteria in this chapter.

5.7 As the definition of materiality is tied to an individual firm's ability to meet the Threshold Conditions on an ongoing basis and comply with the Fundamental Rules, 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. However, each firm should also take reasonable steps to come to an informed view as to the materiality of the arrangement on it as an individual firm.

Timing and frequency of materiality assessments

5.8 Firms are responsible for assessing the materiality of their outsourcing and third party 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 a significant organisational change at the service provider or a material sub-outsourced service provider takes place that could materially change the nature, scale, and complexity of the risks inherent in the outsourcing arrangement, including a significant change to the service provider's ownership or financial position..

5.9 Where a firm expects an outsourcing or third party arrangement to become material in the future, it should take reasonable steps to ensure that it can comply with all applicable expectations for material outsourcing arrangements in Chapters 6 to 10 on or before the materiality threshold is crossed. If a non-material outsourcing or third party arrangement becomes material due to a severe but plausible scenario, such as a pandemic, firms should consider whether additional measures to safeguard their operational resilience are warranted, such as revisions to contractual provisions.

Criteria for assessing materiality

5.10 Firms should develop their own processes for assessing materiality as part of their outsourcing or third party risk management policy (see Chapter 4). However, to ensure consistency across firms' assessments, the PRA expects firms to take into account certain criteria, as set out below.

Criteria that will generally render an outsourcing arrangement automatically material

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

- financial stability of the UK;

- firms':
  - ability to meet the Threshold Conditions;
  - compliance with the Fundamental Rules;
  - requirements under 'relevant legislation' and the PRA Rulebook;[36]
  - 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:
    i. 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
    ii. requirement not to undermine the 'continuous and satisfactory service to policyholders' in line with Conditions Governing Business 7.2.
  - OCIR and if applicable, resolvability.

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

- entire 'regulated activity', eg portfolio management ;[37] or
- 'internal control' or 'key function', unless the firm is satisfied that a defect or failure in performance would not adversely affect the relevant function.[38] [39]

Other materiality criteria to take into account

5.13 The PRA expects firms to have regard to all applicable criteria in Table 5 below, both individually and in conjunction, when assessing the materiality of an outsourcing or third party arrangement not otherwise covered by paragraphs 5.8 and 5.9. Although in practice many material outsourcing and third party arrangements involve ICT products or services (eg cloud), the presence of a given ICT product or service does not, in itself, automatically render an outsourcing arrangement material.

Table 5: 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	• business continuity, operational resilience, and operational risk, including: - conduct risk;

36 Relevant legislation' has the same meaning as in the Information Gathering Part of the PRA Rulebook.
37 See also paragraphs 62 and 63 of the EBA Outsourcing Guidelines regarding the outsourcing of entire regulated (banking) activities to service providers located outside the EEA.
38 For full definition, see 'internal controls' in the Glossary Part of the PRA Rulebook.
39 Key function holder means any person who is responsible for discharging a key function.

inadequate performance on the firm's:	- ICT risk;[40] - legal risk; and - reputational risk.[41]
	• ability to: - comply with legal and regulatory requirements; - conduct appropriate audits of the relevant function, service, or service provider; and - identify, monitor, and manage all risks.
	• obligations under - the PRA Rulebook; - the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity of the institution or payment institution and its clients, including but not limited to GDPR and the Data Protection Act 2018.
	• 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

5.14 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'. 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 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 Fundamental Rule 7.

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

- 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). In some circumstances, it might be appropriate to make a notification before a final provider has been selected. An example of this is if a firm is planning a major migration programme and is still trying to select a provider from a shortlist.

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

40 As defined in the EBA 'Guidelines on ICT and security risk management'.
41 In line with the definition of 'operational risk' in the PRA Rulebook, insurers should consider reputational risks in addition to and separately from operational risk.

5.17 Although Notifications 2.3(1)(e) only apply to material outsourcing arrangements, material non-outsourcing third party arrangements may constitute 'information of which the PRA would reasonably expect notice' within the meaning of Fundamental Rule 7 and Senior Manager Conduct Rule/Conduct Standard 4.[42] Consequently, the PRA expects firms to bring these arrangements to its attention in a similar manner and timeframe to that set out in paragraphs 5.14–5.16. Firms may elect to develop a single internal framework for notifying the PRA of material outsourcing and material non-outsourcing third party arrangements to the PRA.

Due diligence

5.18 The PRA expects firms to conduct appropriate due diligence on the potential service provider before entering into an outsourcing arrangement, and to identify a suitable alternative or back-up providers where available. If no alternative or back-up providers for a material outsourcing arrangement are available, firms should consider alternative business continuity, contingency planning, and disaster recovery arrangements to ensure they can continue providing relevant important business within their impact tolerances in the event of material disruption at their chosen service provider (see Chapter 10).

5.19 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;
- ICT controls and security; and
- sub-outsourced service providers, if any, that will be involved in the delivery of important business services or parts thereof.

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

- have the authorisations or registrations required to perform the service;
- comply with GDPR, the Data Protection Act, and other applicable legal and regulatory requirements on data protection;
- can demonstrate certified adherence to recognised, relevant industry standards;
- can provide, where applicable and upon request, relevant certificates and documentation (eg data dictionaries); and
- have the ability and capacity to provide the service that the firm needs in a manner compliant with UK regulatory requirements (including in the event of a sudden spike in demand for the relevant service, for instance as a result of a shift to remote working during a pandemic). A 'general' track-record of previous performance may not be sufficient evidence by itself.

42 Senior Manager Conduct Standard/Rule 4: You must disclose appropriately any information of which the FCA or the PRA would reasonably expect to have notice.

Risk assessment

5.21 In line with Risk Control 3.4(2) and Risk Management 3.1, firms should, in a proportionate manner, assess the potential risks of all third party arrangements, including outsourcing arrangements, regardless of materiality. 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 and integrity of sensitive data and/or availability of service provision (see Chapter 10); 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, including as a result of an economic downturn ('step-in' risk).[43]

5.22 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.

5.23 A firm's risk assessment should balance any risks that 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

5.24 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;

  - fourth party/supply chain dependencies, for instance, where multiple otherwise unconnected service providers depend on the same sub-contractor for the delivery of their services;

  - arrangements with service providers that are difficult or impossible to substitute; and/or

  - concentration of outsourcing and other third party dependencies in a close geographical location, such as one jurisdiction. This type of concentration may arise even if a firm uses multiple, unconnected third party service providers, for instance, a business process outsourcing or offshoring hub.

[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 Solvency II Delegated Regulation (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, each outsourced service should be appropriately documented, although not necessarily in a separate agreement.

6.3 Firms should ensure that written agreements for non-material outsourcing arrangements include appropriate contractual safeguards to manage and monitor relevant risks. Moreover, 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.

Material outsourcing agreements

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

- a clear description of the outsourced function, including the type of support services to be provided;
- the start date, next renewal date, end date, and notice periods regarding termination for the service provider and the firm;
- the 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, processed, or transferred, including the possible storage location, and a requirement for the service provider to give reasonable notice to 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 (this may be by reference to 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 or adverse 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. For the firm, these should take account of their impact tolerances for important business services. Where appropriate, both parties should commit to take reasonable steps 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 ICT security requirements, specifications of firms' data lifecycles, 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. Firms may elect to limit contractual termination rights to situations such as:

  - material breaches of law, regulation, or contractual provisions;

  - those that create risks beyond their tolerance; or

  - those that are not adequately notified and remediated in a timely manner.

6.5 If an outsourced service provider in a material outsourcing arrangement is unable or unwilling to contractually facilitate a firm's compliance with its regulatory obligations and expectations, including those in paragraph 6.4, firms should make the PRA aware of this.

7 Data security

7.1 In this chapter, the term 'data' should be interpreted very broadly to include confidential, firm sensitive, and transactional data. It may also cover open source data (eg from social media) collected, analysed, and transferred for the purposes of providing financial services as well as the systems used to process, transfer, or store data. The expectations in this chapter apply to material outsourcing arrangements and other third party arrangements that involve the transfer of data with third parties in line with the EBA ICT GL. This chapter should also be interpreted consistently with requirements under data protection law.

7.2 Where a material outsourcing or third party agreement involves the transfer of or access to 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.

7.3 Building on General Organisational Requirements 2.4 (banks) and Article 274(e) of the Solvency II Delegated Regulation, where a material outsourcing or third party 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 the relevant data and their impact (legal, reputational, etc.);
- agree an appropriate level of data availability, confidentiality, and integrity; and
- if appropriate, obtain appropriate assurance and documentation from third parties on the provenance or lineage of the data to satisfy themselves that it has been collected and processed in line with applicable legal and regulatory requirements.

7.4 Some risks relating to data that the PRA expects firms to consider include but are not necessarily limited to unauthorised access, loss, unavailability, and theft.

Data classification

7.5 Firms are responsible for classifying their data. While the PRA does not prescribe a specific taxonomy for data classification, it expects firms to implement appropriate, risk-based technical and organisation measures to protect different classes of data (eg confidential, client, personal, sensitive, transaction) when:

- developing and implementing their outsourcing policy and other relevant policies and strategies in paragraph 4.10 (business continuity, contingency planning, disaster recovery, ICT, information security, operational resilience, OCIR, and risk management); and
- sharing data with third parties, including but not limited to as part of an outsourcing arrangement.

Data location

7.6 As noted in Chapter 10, the PRA recognises the potential benefits for operational resilience of firms using cloud technology to distribute their data and applications across multiple, geographically dispersed availability zones and regions. This approach can strengthen firms' ability to respond and

recover from local operational outages faster and more effectively, and enhance their ability to cope with fluctuations in demand.

7.7 The PRA also recognises the potential negative consequences of restrictive data localisation requirements on firms' innovation, resilience, and costs. None of the expectations in this SS and in particular this section should be interpreted as explicitly or implicitly favouring restrictive data localisation requirements.

7.8 However, the PRA expects firms to adopt a risk-based approach to the location data that allows them to simultaneously leverage the operational resilience advantages of outsourced data being stored in multiple locations and manage relevant risks, which may include:

- legal risks stemming from conflicting or less developed relevant legal or regulatory requirements in one or more of the countries where the data may be processed;

- challenges to firms', the Bank's, and PRA's ability to access firm data in a timely manner if required (eg as part of their enforcement, resolution, or supervisory functions) due to local law enforcement, legal, or political circumstances; and

- other potential risks to the availability, security, or confidentiality of data, for instance, high risk of unauthorised access or ICT risks stemming from inadequate data processing equipment.

7.9 As part of their due diligence and risk assessment in the pre-outsourcing phase, firms should identify whether their data could be processed in any jurisdictions that are outside their risk tolerance and, if so, bring this to the attention of the third party when negotiating the contractual arrangement in order to discuss adequate data protection and risk mitigation measures.

Data security

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

7.11 The PRA expects firms to implement robust controls for data-in-transit, data-in-memory, and data-at-rest. Depending on the materiality and risk of the arrangement, these controls may include a range of preventative and detective measures, including but not necessarily limited to:

- configuration management. This is a particularly important measure, as for example, in the context of cloud, misconfiguration of cloud services can be a major cause of data breaches;

- encryption and key management;

- identity and access management, which should include stricter controls for individuals whose role can create a higher risk in the event of unauthorised access, (eg systems administrators). Firms should be particularly vigilant about privileged accounts becoming compromised as a result of phishing attacks and other leaking or theft of credentials in line with paragraph 31 of the EBA ICT GL;

- the ongoing monitoring of 'insider threats', (ie employees at the firm and at the third party who may misuse their legitimate access to firm data for unauthorised purposes maliciously or

inadvertently). The term 'employee' should be construed broadly for these purposes and may include contractors, secondees, and sub-outsourced service providers (see Chapter 9);

- 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, provided that access to the data by the firm or PRA is no longer required (see Chapters 8 and 10). When deciding when to delete data, firms will need to consider their obligations under data protection law and their potential data retention obligations.

7.12 Where data is encrypted, firms should ensure that any encryption keys or other forms of protection are kept secure by the firm or outsourcing provider. The data protected by encryption (although not necessarily the encryption keys themselves) should be provided to the PRA in an accessible format if required, in accordance with Fundamental Rule 7 and other potentially relevant regulatory requirements.

7.13 The ability of service providers to respond to customer-specific data security requests may vary depending on the service being provided. Generally, the more standardised the service, the more difficult it might be for the service provider to accommodate these requests. The PRA's focus is on the overall effectiveness of the service provider's security environment, which should allow firms to meet their regulatory and risk management obligations and be at least as effective as their in-house security environment. As long as service providers can provide assurance that this is the case, the PRA does not have specific expectations around customer-specific requests.

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 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, banks or insurers)[44]	Outsourcing (all or material)	Statutory Power	Description	Directly applicable to service providers as well as firms? (Yes or No)
All	All	Section 165A 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.'[45]	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
All	All	Section 166(2)(b) FSMA	The PRA can require any member of the authorised person's group to provide information or produce documents with respect to any matter.	No
Banks	All	Section 3A of the Banking Act 2009 (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

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. 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

44 The term 'All' in Tables 6 and 7 includes all PRA-regulated firms, including credit unions and NDFs.
45 See SoP 'The financial stability information power', June 2014: www.bankofengland.co.uk/prudential-regulation/publication/2014/the-financial-stability-information-power-sop.

All	Material	Information Gathering 2.2 and 3.3	Firms must take reasonable steps to ensure their suppliers under material outsourcing arrangements: • deal with the PRA in an open, co-operative and timely way in the discharge of the PRA's functions under relevant legislation; and • 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, the Bank (as a resolution authority), and any other person appointed by firms or the Bank and PRA, with full access and unrestricted rights for audit and information to enable firms to:

- comply with their legal and regulatory obligations; and
- monitor 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 may include, where appropriate, the service provider's policies, processes, and controls on data ethics, data governance, and data security;
- the results of security penetration testing carried out by the outsourced service provider, or on its behalf, 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.

8.5 The PRA considers that it is not sufficient for firms merely to negotiate adequate access, audit, and information rights; these must also be used when appropriate. The purpose of the rights outlined in this chapter is to support firms' identification, assessment management, and mitigation of any identified risks relating to a material outsourcing arrangement. The appropriate exercise of these rights is key to providing the assurance that such an arrangement is being provided as agreed with the outsourced provider and in line with regulatory requirements.

Pooled audits and third party certificates and reports

8.6 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.

8.7 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).

8.8 Firms can choose any appropriate audit method as long as it enables them to 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 that 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

8.9 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 audit reports meet the expectations in Table 8.

Table 8: Expectations for certificates and audit reports

Scope	• Key systems and controls identified by the firm (eg applications, infrastructure, data centres, and processes). • Compliance with relevant requirements (eg PRA rules and EBA Outsourcing GL).
Content	• Up-to-date information. • Reviewed regularly to reflect updates to the service provider's controls, new or revised legal, regulatory requirements, or expectations and recognised standards. • Where available, the PRA encourages the use of online, real-time reporting tools.
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. • Be performed in line with recognised standards.

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

- request additional, appropriate, and proportionate information if such a request is justified from legal, regulatory, or risk management perspectives; and
- perform onsite audits (individual or pooled) at their discretion.

Onsite audits

8.11 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. Such notice should include the location and purpose of the visit and the personnel that will participate in the visit;

- 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).

8.12 Certain types of onsite audit create may an unmanageable risk for the environment of the provider or its other clients, for example, by impacting service levels or the confidentiality, integrity, and availability of data. In such cases, the firm and the service provider may agree alternative ways to provide an equivalent level of assurance, for instance, through the inclusion of specific controls to be tested in a report or certification. The PRA expects that firms should retain their underlying right to conduct an onsite audit. For material outsourcing arrangements, the PRA would expect the firm to inform their supervisor if alternative means of assurance have been agreed.

Pooled audits

8.13 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 regard to audit methods among firms.

8.14 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 GL 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. The PRA Rulebook also explicitly acknowledges that a service provider may perform ‘a process, a service or an activity which would otherwise be undertaken by the firm itself […] directly or by sub-outsourcing’. 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.

Firms' oversight of sub-outsourcing

9.3 The PRA expects firms to assess the relevant risks of sub-outsourcing before they enter into an outsourcing agreement. It is important that firms have visibility of the supply chain, and that service providers are encouraged to facilitate this 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, including their ability to remain within impact tolerances during operational disruption. Firms should also consider whether extensive sub-outsourcing could compromise their ability to oversee and monitor an outsourcing arrangement.

9.5 Firms should assess whether sub-outsourcing meets the materiality criteria set out in Chapter 5, which includes the potential impact on the firm's operational resilience and the provision of important business services. Firms should only agree to material 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) (insurers); 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 to the service provider.

9.6 Firms should ensure that the service provider has the ability and capacity on an ongoing basis to appropriately oversee any material sub-outsourcing in line with the firm's relevant policy or policies. This includes establishing that the service provider has in place robust testing, monitoring, and control over its sub-outsourcing.

9.7 If the proposed material sub-outsourcing could have significant adverse effects on a material outsourcing arrangement or would lead to a substantive increase of risk, the firm should exercise its right to object to the material sub-outsourcing and/or terminate the contract.

9.8 There may be situations where the same service provider has a direct contractual relationship with a firm and is also a sub-outsourced service provider to that firm. An example might be a firm that has an agreement with a cloud service provider that provides services to one or more software vendors used by that firm. In those situations, where appropriate, firms may leverage their direct contractual relationship with that service provider to assess its resilience in respect of all the services it relies on that provider for, including as a material sub-outsourced service provider.

Written agreement

9.9 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 specifying 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 material sub-outsourcing or significant 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).

Termination Rights
Some non-exhaustive examples of situations where a firm may consider exercising its contractual right to terminate the outsourcing agreement include if: • without notifying the firm, the outsourced service provider changed its list of material sub-outsourcers to include a firm that had a significant history of data breaches and operational outages; • a material sub-outsourced provider has failed to grant the firm, the Bank, and/or the PRA equivalent access, audit, and information rights; • a significant incident at a sub-outsourcer caused extensive and unmanageable operational disruption to a firm so that it could no longer stay within its impact tolerances for important business services; • a sub-outsourced service provider repeatedly causes the outsourced provider to fail to meet KPIs and service expectations that have been agreed with the firm; • a sub-outsourced service provider enters into insolvency proceedings or other legal proceedings that may materially impact the delivery of its services; and • actions taken following an incident fail to deliver appropriate remediation.

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 the Bank to assess the effectiveness of service providers' business continuity plans. In particular, they should be able to assess 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-premises and public cloud data centres);
- multiple or back-up vendors;
- retaining the ability to bring data or applications back on-premises; and/or
- any other viable approach that can achieve and promote an appropriate level of resiliency.

10.6 There is no hierarchy or one-size-fits-all combination of cloud resiliency options. The optimal option or combination of options will depend on various factors, including but not limited to the:

- size and internal organisation and the nature, scope, and complexity of the firm's activities (proportionality);
- potential impact of the outsourcing arrangement on the provision of important business services by the firm (materiality); and
- the relative costs and benefits of different options, taking into account the risks that failure or prolonged operational disruption may pose to UK financial stability or the safety and soundness of the firm, and (for insurers) policyholder protection.

10.7 If a significant firm wants to outsource its core banking platform to the cloud, the PRA may expect it to adopt one or more of the most resilient options available to maximise the chances to maintain its resilience in the event of a serious outage. Conversely, if a non-significant firm wishes to

do so, then a less resilient but nonetheless robust option or combination of options could be appropriate.

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

10.9 In line with Fundamental Rule 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. This is so all relevant internal and external stakeholders, including the Bank, PRA, FCA, other international regulators, and, if relevant, the service providers themselves, are informed in a timely and appropriate manner.

Stressed exits

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

10.11 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).[46]

10.12 The PRA does not prescribe or have a preferred form of exit in stressed scenarios. Its focus is on the outcome of the 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.

10.13 The PRA does, however, expect firms to identify viable forms of exit in a stressed exit scenario, and give meaningful consideration to those that best safeguard their operational resilience, which may include but not be limited to:

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

10.14 The PRA expects firms to consider the available tools that could help facilitate an orderly stressed exit from a material outsourcing arrangement. Such 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.

10.15 The PRA recognises that, in an intragroup outsourcing context, firms' exit options might be more limited than in other scenarios. This is particularly true for third-country branches, which are unable to enter into standalone contractual arrangements with third parties. Nevertheless, the PRA

46 In intragroup outsourcing scenarios, the stressed parts of these exit plans can also help facilitate compliance with Operational Continuity 4.4 where applicable.

expects third-country branches to take reasonable steps to try and identify options, however limited, to maintain their operational resilience.

10.16 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 or escrow arrangements), allowing for continued use of a service or technology for a transitional period following termination.

Governance of business continuity plans and exit plans

10.17 Firms should begin to 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 which, if breached, may trigger an exit (both stressed and non-stressed).

10.18 Firms should evaluate what would be involved in delivering an effective stressed exit and use this to formulate plans for such an exit, assisting them to identify any assets and skills required. As soon as practically possible, firms should seek to test the stressed exit plans to ensure they are functional and meet expectations around impact tolerances and costs, etc.

10.19 Once an outsourcing arrangement has been implemented, firms should test their business continuity and exit plans on a risk-based approach. Where possible and relevant, this testing should align to, support, or even be a component of firms' scenario testing under Operational Resilience – CRR Firms 5 and Operational Resilience – Solvency II Firms 5. For instance, one of the severe but plausible scenarios that firms may select for this testing could involve a failure or disruption at a third party or their supply chain, based on previous incidents or near misses within the organisation, across the financial sector and in other sectors and jurisdictions. In line with paragraph 6.4 and the FSB Effective Practices, firms and third parties should commit to support the testing of such plans.

10.20 For firms subject to the CBEST framework, the CBEST implementation guide notes that 'malicious Insider and Supply Chain Scenarios are a feature of the threat landscape for many firms. These scenarios should always be analysed and discussed during CBEST'. Where required, these firms 'should plan in advance the involvement of staff and third parties to increase the reality of assessment'.[47]

10.21 Consistent with the EBA ICT GL, firms should also update their business continuity and exit plans with lessons learned from these tests, including with new risks and threats identified and changed recovery objectives and priorities (if any).

47 https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide.

10.22 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.

10.23 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.

10.24 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 that may be caused or increased by the actual testing (eg data theft).

10.25 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-premises environments and the cloud).

TABLE 9: Contingency planning in outsourced insurance policy administration

Contingency planning – observed best practice in insurers
In 2019, the PRA conducted a thematic review of insurers' contingency plans in the event of the failure of a material outsourced service provider providing policy administration services. The PRA identified the following good practices, which insurers may wish to consider when conducting their contingency planning: • Proposals to act collaboratively with other insurers who share a common outsourcer, in the event of outsourcer failure. • Evidence of awareness of the challenges of utilising step-in rights where there are shared services. • Evidence that the contingency plans had been signed off at an appropriately senior level given the criticality of the outsourced service. • A list of named contacts and details of individuals and teams responsible for implementing the contingency plan.

- Evidence that contractual provisions took contingency planning into consideration, for instance, by including provisions on:
  - step-in rights;
  - provisions to transfer employees of the service provider to the insurer under the Transfer of Undertakings (Protection of Employment) Regulations (TUPE); and
  - access by the insurer to necessary data and systems of the service provider.
- Consideration of a range of scenarios in which a contingency plan may need to be used, including:
  - financial and/or operational failure of the service provider; and
  - if the service provider enters or is at risk of entering into administration or liquidation.
- An assessment of the:
  - substitutability of the service being outsourced;
  - availability of alternative service providers;
  - 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
  - time it would take to implement a given contingency plan.
- Evidence that key assumptions made in the assessments have been tested.