SLAUGHTER AND MAY/

CLIENT BRIEFING

MAY 2021

OUTSOURCING AND THIRD PARTY RISK MANAGEMENT

THE PRA'S STANCE ON RISKS AND CONTROLS

What's new?

In March 2021, the PRA published a Policy Statement on outsourcing and third party risk management (PS7/21) and an accompanying Supervisory Statement (SS2/21) which '*clarifies, develops, and modernises*' longstanding regulatory requirements and expectations applying to financial institutions in this area.

SS22/21 contains provisions – to be applied in line with the principle of proportionality – relating to the lifecycle of firms' outsourcing and certain non-outsourcing third party arrangements. They apply to UK banks, building societies, PRA-designated investment firms, (re)insurance firms and groups in scope of Solvency II, as well as UK branches of overseas banks and insurers. The usual array of measures are addressed: from governance and record keeping, the oversight of sub-outsourcing arrangements, rights of access, audit, and information, as well as business continuity and exit planning, some of which we explore in more detail below.

Non-outsourcing third party arrangements

The PRA's overarching aim in setting the expectations in SS2/21 is for firms to apply adequate governance and controls to all third party dependencies that might impact the PRA's statutory objectives. This could include arrangements that '*support the provision of important business services or carry a high level of risk'*. As such, it confirms what we have assumed for some time: that third party operational dependencies which may not meet the definition of an 'outsourcing' should be risk-managed on essentially the same basis.

The SS notes: '*the PRA maintains that certain non-outsourcing third party arrangements might be highly relevant to the PRA's objectives; for instance, if they support the provision of important business services. Therefore, the SS sets out the expectation that firms should assess the materiality and risks of all third party arrangements using all relevant criteria in Chapter 5 of the SS, irrespective of whether they fall within the definition of outsourcing. Firms should attach greater importance to the dependencies and risks that their outsourcing and third party arrangements create than to specific definitions'*.

Once a firm has concluded that a non-outsourcing, third party arrangement is 'material' or 'high risk,' having consulted the relevant criteria in Chapter 5 of the SS, it must implement effective, risk-based controls which '*do not have to be the same as those that apply to outsourcing arrangements*,' but should be '*equally robust and commensurate to the materiality or risk exposure of the arrangement'*.

SS2/21 does not present the complete picture of requirements. There are several other PRA rules, all listed helpfully in the SS (including the Fundamental Rules and the Operational Resilience Part of the PRA Rulebook), which apply to and govern the management of third party arrangements, irrespective of whether they fall within the definition of outsourcing. Examples might include the design and build of an on-premise IT platform, the purchase of data collated by a third party or the purchase of 'off the shelf' machine learning models. A cloud arrangement will not automatically constitute an outsourcing under the PRA's definition, but should nonetheless be subject to risk-based controls that are commensurate to its materiality.

Firms can opt to implement a '*holistic, single third party risk management policy covering outsourcing and non-outsourcing third party arrangements*' or they can have separate but consistent and suitably risk-based policies applying to each subset.

Interaction with EBA Guidelines and other standards

SS2/21 will ultimately constitute '*the primary source of reference for UK firms when interpreting and complying with PRA requirements on outsourcing and third party risk management*,' though in practice, it is unlikely to be the *only* source. There has been a rising tide of guidelines and recommendations for firms on outsourcing, third party risk management, cloud outsourcing and information and communication technology (ICT) risk management emerging from UK, EU and other international supervisory authorities and other standard setters.

Other UK standards:

Assessing the materiality of an outsourcing or other third party arrangement under SS2/21

Firms should determine the materiality of all third party arrangements using relevant criteria in Chapter 5.

It is noted that: '*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;

- safety and soundness;

- Operational Continuity In Resolution and if applicable, resolvability.'

Generally speaking, an outsourcing arrangement will be classified as 'material' if the service being outsourced involves an '*entire 'regulated activity"* (portfolio management is provided as an example) or an '*internal control or key function*'.

Even if none of these criteria apply, firms are expected to consult a list of factors in the SS to further assess the materiality of a particular outsourcing or third party arrangement.

PS7/21 and SS2/21 are designed to '*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 'Operational resilience'. The latter were published on the same day as the materials on outsourcing and form '*a helpful lens for firms to assess how they should monitor their outsourcing and third party arrangements and establish end-to-end resilience for their important business services*'.

EBA Guidelines and other international standards:

SS2/21 implements the European Banking Authority (EBA) Outsourcing Guidelines, which were finalised in February 2019 and began to apply on 30 September last year, and parts of the EBA ICT Guidelines. It has also '*taken into account*' various international standards including the Basel's 'Principles for operational resilience'; the FSB's 'Effective Practices for Cyber Incident Response and Recovery'; and IOSCO's 'Principles on Outsourcing', some of which are stil in draft form.

The PRA does not expect firms to comply with any EU Guidelines that came into effect after the end of the implementation period - such as the EIOPA Cloud Guidelines, the EIOPA ICT Guidelines or the ESMA Guidelines on outsourcing to cloud service providers - and it has not formally implemented them in the SS, but it considers that the expectations in the SS are '*at least equivalent to them in effectiveness and substance'*. All relevant EU Guidelines continue to apply to the European operations of UK firms and to the activities undertaken in the EU by firms that also have a UK presence. Firms that are subject to SS2/21 will not need to comply with the EBA's deadline of 31 December 2021 to review and update legacy outsourcing arrangements of critical or important functions in line with the Outsourcing Guidelines, though that timeline will continue to impact firms regulated in the EU.

SS2/21 is '*not materially divergent*' from the EBA Guidelines, but where the PRA's expectations are more granular than equivalent sections in the EBA Outsourcing or ICT Guidelines, the PRA considers that this results '*in clearer, more consistent policy that will provide firms with greater regulatory certainty'*. Consistent with the EBA Guidelines, 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*'. This means that a one-off purchase, such as a software licence, would not be an outsourcing, but it might still be a third party arrangement that triggers the requirement for appropriate risk-based controls and - depending on the underlying cloud infrastrucutre – could require the management of concentration risks.

The criteria for identifying a '*material outsourcing*' is substantively aligned to the equivalent EBA term of '*critical or important outsourcing*' with a '*few justified exceptions*' such as those that reference the PRA's requirements on operational resilience. Material/critical/important arrangements generate more onerous requirements.

Advance notification of material arrangements

The PRA expects advance notification of material third party arrangements in a similar manner and timeframe as it would a material outsourcing arrangement (notwithstanding that the relevant PRA rule Notifications 2.3(1)(e) applies only to the latter). This is because material third party arrangements that do not meet the outsourcing definition may constitute '*information of which the PRA would reasonably expect notice*' within the meaning of Fundamental Rule 7 and Senior Manager

Intragroup and branch arrangements

SS2/21 provides more granularity than the EBA Guidelines on the application of the principle of proportionality to intragroup outsourcing arrangements, as apparently requested by respondents to the underlying PRA consultation. The details do not change the fundamental premise that intragroup arrangements are not to be treated as inherently less risky than arrangements with third parties outside a firm's group; but there is some scope for firms to make pragmatic management adjustments. In certain cases, for example, firms may rely on business continuity, contingency, and exit plans developed at the group level. The relevant requirements apply proportionately depending on the level of the recipient group's 'control and influence' over the entity that is providing the outsourced service.

The PRA has also set out its approach to outsourcing requirements and expectations for the UK branches of overseas (third-country) firms. At a minimum, it will expect those branches to compile a list of their intragroup outsourcing arrangements, identifying those deemed material. Any such arrangement will need to be documented in a written agreement that specifies expected service levels and key performance indicators. There should also be appropriate monitoring and oversight, as well as effective processes and mechanisms for escalating any concerns or issues to the firm or group.

Conduct Rule 4. In certain cirucmances the PRA will expect to be brought into the loop before a final service provider has been selected.

Sub-outsourcing

Firms are responsible for ensuring that third party service providers appropriately manage any material sub-outsourcing. The PRA does not expect firms to directly monitor fourth parties in all circumstances, but the potential impact of large, complex sub-outsourcing chains on firms' operational resilience will need to be considered.

Negotiating with suppliers

An imbalance in negotiating power between a recipient firm and a dominant service provider is not, notes the PRA, justification for a firm to accept clauses and terms that do not meet legal or regulatory expectations. Firms should make the PRA aware if a service provider in a proposed material outsourcing arrangement is unable or unwilling to '*contractually facilitate*' a firm's compliance with the PRA's requirements.

Rights of audit and access

Firms are at liberty to 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 should be in keeping with the significance of the firm and the materiality of the arrangement (so, a significant firm that outsources an important business service for which it has set a low impact tolerance will require a higher level of assurance.)

Additional guidance has been added to the final text of SS2/21 regarding the conduct of on-site audits. In particular, where an on-site audit could create an unmanageable risk for the environment of the provider or other clients, the firm and service providers should agree alternative ways to provide an equivalent level of assurance while not removing the contractual rights for an on-site audit from the written agreement. For material outsourcing arrangements, the PRA would expect the firm to inform its supervisor if alternative means of assurance have been agreed. Access, audit, and information rights extend, where relevant, to requiring institutions to ensure that third parties agree to share the results of security penetration testing they carry out or which are carried out on their behalf. (In an earlier draft of the SS, the PRA had required that firms ensure they have a right, where relevant, to carry out such penetration testing themselves.)

Location of data

After considering responses to the underlying consultation, the PRA has clarified that it does not favour or wish to impose restrictive data localisation requirements. It expects firms to adopt a risk-based approach to the location data such that they can leverage the operational resilience advantages of outsourced data being stored in multiple locations, whilst at the same time managing the attendant risks.

Exit plans

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. Once arangements are implemented, business continuity and exit plans should be tested using a risk-based approach.

The PRA recognises that firms' exit options might be more limited in an intragroup context, particularly for UK branches of third country firms, but it nonetheless expects all firms to take reasonable steps to identify options, however limited, for maintaining operational resilience.

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 (these may include, multiple or back-up vendors or bringing data or applications back on-premises). Again, the expectations are injected with proportionality: so that if a significant firm wants to outsource its core banking platform to the cloud, the PRA will 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.

Timing

SS2/21 will begin to apply on 31 March 2022. The PRA expects outsourcing arrangements entered into on or after 31 March 2021 to be compliant by that date, but has given firms additional time to review and update pre-existing legacy outsourcing agreements '*at the first appropriate contractual renewal or revision point*' so that they comply with the SS '*as soon as possible on or after Thursday 31 March 2022*'.

CONTACTS

BEN KINGSLEY

PARTNER

T: +44 (0) 7909 684669

E: ben.kingsley@slaughterandmay.com

DUNCAN BLAIKIE

PARTNER

T: +44 (0) 7824 592 902

E: duncan.blaikie@slaughterandmay.com

NATALIE DONOVAN

PSL COUNSEL

T: +44 (0) 7826 872415

E: natalie.donovan@slaughterandmay.com

SELMIN HAKKI

SENIOR PSL

T: +44 (0) 7825 313093

E: selmin.hakki@slaughterandmay.com