EVERSHEDS SUTHERLAND

Read all about it

Outsourcing and third party risk management

The PRA has recently published Policy Statement PS 7/21, which contains the PRA's final Supervisory Statement SS2/21 on "Outsourcing and third party risk management" following on from Consultation Paper CP30/19 in December 2019. In essence, this update is the PRA's latest and definitive position on outsourcing and third party risk management which is intended to (amongst other objectives) implement the European Banking Authority Guidelines on Outsourcing Arrangements ("**EBA Guidelines**") and facilitate greater adoption of cloud and other new technologies.

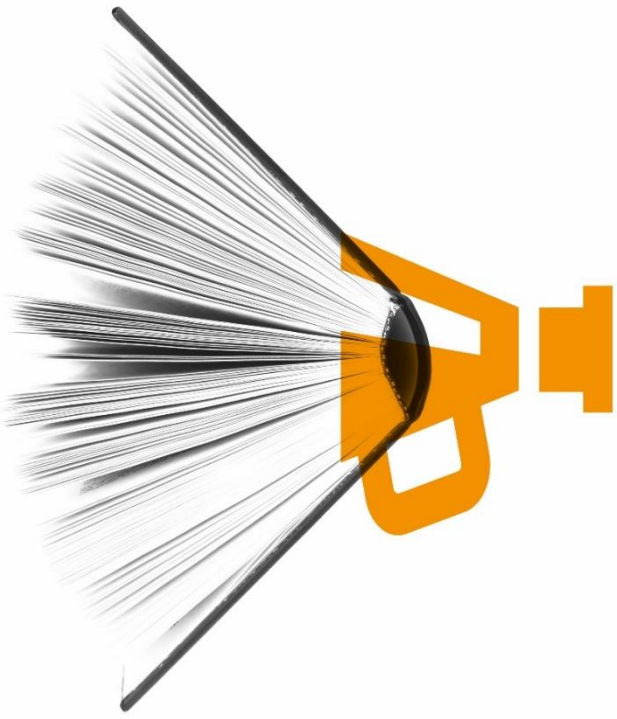
We have highlighted in this briefing some of the key points for financial institutions to be aware of following this update, with a particular focus on changes made as a result of responses to the consultation. This briefing should be read in conjunction with our article on the publication by the Bank of England, PRA and FCA of their final rules and guidance on operational resilience for financial institutions and financial market infrastructures available **here**.

Outsourcing and other third party arrangements

The core requirements of SS2/21 continue to apply to an "outsourcing" that has the now well-rehearsed definition of being an arrangement between the firm and a service provider where the service provider performs a process, service or activity which would otherwise be undertaken by the firm itself. The PRA has helpfully elected not to broaden this definition (as was envisaged as a possibility in CP30/19) to include other third party arrangements that are performed in a prudential context, which we are aware was a suggestion that had caused some concern in the market.

There remains a distinction between an "outsourcing" and a "non-outsourcing third party arrangement". The PRA is (not surprisingly) clear that a non-outsourcing third party arrangement can still be material or high risk and if that is the case then the firm should implement proportionate, risk-based, suitable controls but those are not necessarily the same as those that would apply to an outsourcing arrangement – they should be appropriate to the materiality and risks of the third party arrangement but still as robust as the controls that would apply to outsourcing arrangements with an equivalent level of risk. This is helpful guidance as there continues to be an increased reliance on solutions that are technology heavy but perhaps service or process light. We can expect firms to start to look at their outsourcing and other third party arrangements on a more holistic basis.

There is also helpful clarification that certain arrangements among regulated financial institutions, including between firms and financial market infrastructures do not fall within the definition of outsourcing. These arrangements include clearing, settlement and in particular custody services; to address some recent debate that such arrangements could be caught by the outsourcing regulatory framework.



Intra-group arrangements

The PRA has stated that intragroup arrangements should not be treated as "inherently less risky" than third party arrangements and is subject to the same requirements and expectations. However, it has confirmed that the principles of proportionality may be able to be applied to intra-group arrangements with the result that certain aspects could be managed differently in practice. When exercising proportionality, a firm should take into account their level of "control and influence" over the entity providing the outsourced service.

While an intra-group outsourcing arrangement must always be documented in writing, the PRA has stated that it may be proportionate to adapt certain clauses in outsourcing agreements. One example given (depending on the circumstances) is that the firm may be able to rely on group wide business continuity policies and exit plans.

Data location

Among other clarifications in relation to data security, the PRA has confirmed that it expects firms to "know the location of their data at all times, including when in transit". The PRA suggests that firms identify whether their data could be processed in any high risk jurisdictions outside the risk tolerance in their outsourcing policy. However, the PRA has declined to go so far as to publish a list of what it considers to be a high risk jurisdictions and firms are expected to reach their own conclusions, depending on factors such as the local regulatory requirements in a particular jurisdiction, the ease of accessing the data in a timely manner and other potential risks to the availability, security or confidentiality of data.

On-site audits

The PRA has provided further clarification on their interpretation of the requirement under the EBA Guidelines to have unrestricted rights of audit. In particular, the PRA has acknowledged that there may be certain types of onsite audit which could create an unmanageable risk for the environment of the service provider. In such circumstances, the PRA confirms that it may be appropriate for the firm to agree with the service provider an alternative way of achieving an equivalent level of reassurance. However, it appears that this is very much intended to be an exception to apply in limited circumstances only.

On the challenging topic of penetration testing, helpful guidance has also been provided that rather than firms being expected to pen test the infrastructure of its service providers, what is more relevant is access to the results of the testing that the service provider (or its third party contractors on its behalf) perform on its own technology.

Sub-outsourcing

The PRA has clarified a number of issues around sub-outsourcing including the following:

- the detailed expectations on sub-outsourcing only apply to material sub-outsourcing, to be determined in accordance with the materiality criteria set out in Chapter 5 of SS2/21
- firms are not expected to directly monitor the sub-outsourcing parties themselves provided they can effectively oversee and monitor the outsourcing arrangement as a whole, including by ensuring the service provider appropriately manages the sub-outsourcing

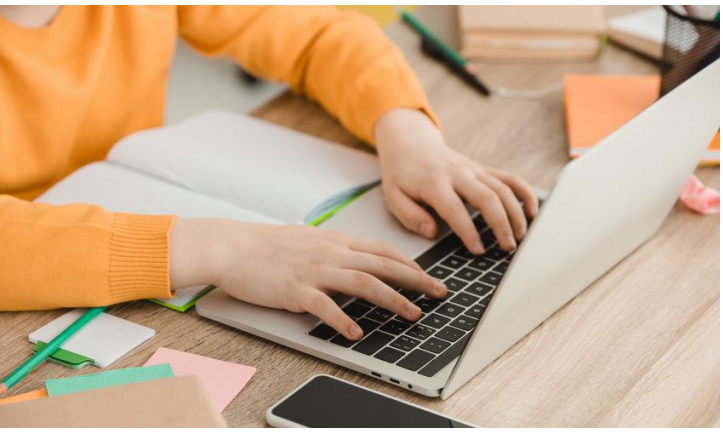
Termination rights

SS2/21 includes some updated guidance for firms on how to approach the topic of termination and the termination rights that are referenced in the EBA Guidelines. The requirements in respect of termination will of course need to be applied on a case by case basis, but in broad terms the language in SS2/21 makes it far easier to apply what are fairly well established market practice termination rights for a third party outsourcing or technology arrangement.

Non-contractual requirements

There are also a number of non-contractual requirements in the context of third party outsourcings which the PRA has drawn out in more detail. In particular, the PRA has clarified a number of points around the notification and record keeping requirements, including the following:

- the PRA considers that, in some circumstances, it may be appropriate to notify it of a planned material outsourcing prior to selection of final service provider. This underlines the requirement to engage with and notify the PRA at an early stage in planned outsourcings – this cannot be stressed enough in current times
- the PRA also expects to be notified of material non-outsourcing third party arrangements which may constitute "information of which the PRA would reasonably expect notice"
- the PRA expects to be made aware in a circumstance where a third party service provider to a material outsourcing is unable or unwilling to include certain terms within the contract which are required by the PRA
- the PRA is going to publish a subsequent consultation setting out proposals for an online centralised portal to be populated by firms with information on their outsourcing arrangements. This would link in with the existing obligations on firms to maintain this internal register of their outsourcing arrangements



Timeline for Compliance

The PRA has confirmed that firms will be expected to comply with the requirements set out in SS2/21 by Thursday 31 March 2022 in respect of outsourcing arrangements entered into on or after Wednesday 31 March 2021. In respect of legacy outsourcing agreements, the PRA expects firms to work towards remediating these contracts at the first appropriate contractual renewal or revision point as soon as possible on or after 31 March 2022.

In welcome news for dual-regulated firms, the FCA has since updated its expectations for FCA-regulated firms who are within scope of the EBA Guidelines, confirming that it no longer expects firms to report to the FCA on their progress towards meeting the EBA-imposed deadline of 31 December 2021 to comply with the EBA Guidelines. Instead, in line with the PRA's approach under SS2/21 and the related rules and guidance on operational resilience, the FCA now expects firms to review any outstanding important or critical arrangements at the first appropriate contract renewal following the first renewal date or revision point and inform the FCA where those arrangements have not been finalised by 31 March 2022.

Simon Gamlin
Partner

T: +44 20 7919 4689

Connect with Simon Gamlin on LinkedIn

Kirstin McCracken
Principal Associate

T: +44 207 919 0851

Connect with Kirstin McCracken on LinkedIn

Nal Townley
Senior Associate

T: +44 20 7919 4654

Connect with Nal Townley on LinkedIn

eversheds-sutherland.com

LON_LIB1\24717888\1