Stand out for the right reasons
Financial Services Risk and Regulation

PRA issues outsourcing and third party risk management requirements

HOT TOPIC
March 2021

Highlight

The PRA has issued its final Supervisory Statement for banks, insurers and third country branches regarding its requirements for firms' management of outsourcing and third party risk.

Having considered responses to CP30/19, the PRA have made targeted revisions to the final policy touching on areas including scope, proportionality, materiality and resilience. They have also replaced timelines under the EBA Outsourcing Guidelines with a new effective date of 31 March 2022 and announced plans to consult on an online portal for firms' outsourcing and third party arrangements.

Summary

On 29 March, following an extended 16 month consultation period (CP30/19), the Prudential Regulatory Authority (PRA) published its final Policy (PS7/21) and Supervisory Statements (SS2/21) on outsourcing and third party risk management, alongside final policy and supervisory statements on operational resilience. While there are no fundamental changes to the approach proposed under CP30/19, the PRA has made targeted revisions to the final policy, including some important updates to timelines versus those under the EBA Outsourcing Guidelines. In modernising the micro-prudential framework for managing outsourcing and third party risk, the PRA's objectives are to:

- facilitate greater resilience and adoption of the cloud and other new technologies
- complement the policy proposals on operational resilience; and
- implement the EBA Outsourcing Guidelines (see: PwC's At a Glance) and relevant sections of the EBA Guidelines on ICT and security risk management.

The final SS comes into effect on 31 March 2022 and is relevant to all:

- UK banks, building societies and PRA-designated investment firms ('banks');
- insurance and reinsurance firms and groups in scope for Solvency II ('insurers'); and
- UK branches of overseas banks and insurers ('third-country branches')

Key areas specific to PRA Regulated Firms

In implementing the EBA Guidelines on Outsourcing and responding to the feedback from CP30/19 the SS introduces a number of key areas of addition, enhancement and/ or clarity that are summarised below:

Proportionality: Firms' approaches to outsourcing and third party risk management should be appropriate to their size, internal organisation, risk profile and the nature, scope and complexity of their activities. This includes systemic significance - firms whose supervisory contact has indicated they are impact category 1 or 2 should consider themselves 'significant' and subject to heightened expectations.

Board engagement on outsourcing: The SS defines responsibilities for boards, including ensuring appropriate and effective risk management systems and strategies, setting outsourcing risk appetite and tolerance levels, as well as understanding firms' reliance on 'critical service providers'.

Expectations for non-outsourcing third party arrangements and materiality: Firms are reminded that non-outsourcing arrangements are still within the scope of the PRA's Fundamental Rules and general requirements and expectations. Firms are now expected to assess the materiality and risks of all third party arrangements, irrespective of whether they fall within the definition of outsourcing, and to implement proportionate, risk-based controls that are as robust as those that would apply to outsourcing arrangements of equivalent materiality or risk.

Materiality versus criticality: The term 'material outsourcing' has been adopted to describe the outsourcing of critical or important functions to avoid confusion with different but partly overlapping terms e.g. 'critical function'.The SS notes additional services likely to be deemed material based on related regulations such as OCIR and requires consideration of whether performance defect or failure could materially impair a firm's operational resilience, i.e. its ability to continue providing important business services.

Contacts

Rakesh Majithia
Partner
T: +44 (0) 78 0302 3856
E: rakesh.majithia@pwc.com

Penny Flint
Partner
T: +44 (0) 78 0385 8309
E: penny.flint@pwc.com

Charles Rodger
Director
T: +44 (0) 78 8431 7642
E: charles.m.rodger@pwc.com

pwc

Greater proportionality for intra-group arrangements: The SS reinforces the EBA's observation that intra-group arrangements are inherently 'no less risky' than those with external third parties ('vendors'), with further guidance provided on how consideration of the level of control and influence and reliance on group policies and procedures can lead to a more proportionate approach to risk management activities. In addition to outlining implications for due diligence, contracting, oversight, business continuity, contingency and exit planning, the SS also encourages firms to consider if they can leverage elements of their OCIR record-keeping and end-to-end mapping of important business services under Operational Resilience.

Outsourcing agreements: The SS introduces a new expectation that requires firms to alert the PRA when a third party service provider is unable or unwilling to include required terms within material outsourcing agreements.

Extension of approach to substitutability: The SS extends the EBA's approach to substitutability, requiring business continuity and exit plans to be developed during the pre-outsourcing phase and use of due diligence activities to support identification of alternate service providers.

Sub-outsourcing and materiality: The SS provides greater clarity on the PRA's expectations for managing sub-contractors/ fourth parties, with requirements now only applicable to material sub-outsourcing and firms encouraged to leverage any direct contractual relationships they may have with these providers to assess their resilience. When entering into a material outsourcing arrangement, firms are also reminded that they should continue to consider the impact of large, complex sub-outsourcing chains on their operational resilience.

Extension of concentration risk requirements: In addition to assessing and managing over-reliance on third parties, firms are required to assess concentration risks across; arrangements with 'closely connected' providers, fourth party/ sub-contractor dependencies and impossible or difficult to substitute providers. Firms are also now required to consider concentrations of outsourcing and third parties in close geographical locations. The SS emphasises the importance of managing over-reliance on third parties and concentration risk or 'vendor lock-in' at both the firm and group level.

Expanded focus on data security: The SS adopts EBA ICT Guidelines principles in extending data security requirements to all third party arrangements, with further guidance on the 'shared responsibility model' for cloud arrangements, data classifications and expectations for risk-based approaches to data classification, location and security. The PRA expects firms to adopt approaches that enable them to simultaneously leverage the operational resilience advantages of data being stored in multiple locations and manage relevant risks.

Notification requirements: The SS reminds firms of existing notification requirements and the need for prior, timely notifications when 'entering, or significantly changing, a material outsourcing arrangement'. Firms are also expected to bring material non-outsourcing arrangements to the PRAs attention, where these may constitute 'information of which the PRA would reasonable expect notice'. For certain arrangements, including major migration programmes, firms are also encouraged to consider making notifications before a final provider has been selected.

Business continuity and contingency: The SS aligns the implementation and testing of business contingency plans to firms' impact tolerances for important business services, as set out in SS1/21. Firms should also ensure they have 'effective crisis communication measures' for informing all relevant internal and external stakeholders in the event of a disruption or emergency.

Exit strategies and plans: Firms are expected to have exit strategies and plans that provide for all scenarios and to periodically test and update these based on developments that may impact the feasibility of exit, e.g. new technology tools. The SS continues to place particular emphasis on stressed exits to provide a last resort mitigation strategy where disruption cannot be managed by other business continuity measures. Although not prescriptive in terms of form of exit, the PRA expect firms to focus on outcomes and to identify viable forms of exit in a stressed scenario, giving meaningful consideration to those that best safeguard their operational resilience. They also encourage firms to actively consider temporary measures to help ensure ongoing provision of important business services following a stressed exit, allowing for continued use of a service or technology for a transitional period post-termination.

Third country branches: The SS diverges from the EBA Outsourcing Guidelines by treating the provision of services by EU firms to their branches as outsourcing. However, the SS recognises the need to apply a proportionate approach to these arrangements and allows firms to place reliance on activities performed at a group level, e.g. materiality, due diligence, risk assessments, contracting, oversight and business continuity and exit planning.

Applying a risk-based, outcomes-based approach to access, audit and information rights: While continuing to advocate an outcomes- and risk-based approach, the SS recognises that certain types of on-site audit may create unmanageable risk. In these instances, they require firms to agree equivalent levels of assurance, while still maintaining contractual rights for on-site, and to inform their supervisors if alternative means of assurance have been agreed for material outsourcing.

Outsourcing Registers and online portals: The PRA reminds firms that the EBA Outsourcing Guidelines already require banks to maintain a register of their cloud outsourcing arrangements and that this should be subsumed into broader register of all outsourcing requirements from 31 December 2021. The PRA is planning a follow-up consultation setting out detailed proposals on an online portal for firms' outsourcing and third party arrangements. Meantime, firms are encouraged to continue following existing record-keeping requirements.

Next steps

Outsourcing arrangements entered into on or after 31 March 2021 should meet the expectations in the SS by 31 March 2022. Legacy outsourcing agreements entered into before 31 March 2021 need to be remediated at the first appropriate contractual renewal or revision point to meet the expectations in the SS as soon as possible on or after Thursday 31 March 2022.

Firms will need to review the impact of new or changed requirements introduced under this SS and incorporate these into their existing frameworks and remediation activities, allowing sufficient time for this, recognising resourcing implications and key external dependencies.

Contacts

Rakesh Majithia
Partner

T: +44 (0) 78 0302 3856
E: rakesh.majithia@pwc.com

Penny Flint
Partner

T: +44 (0) 78 0385 8309
E: penny.flint@pwc.com

Charles Rodger
Director

T: +44 (0) 78 8431 7642
E: charles.m.rodger@pwc.com

www.pwc.co.uk/fsrr