BANK OF ENGLAND

Simon Morley
Director
Financial Market Infrastructure Division
Supervision
T 020 3461 7881

17 September 2021

Dear CEO

Supervisory expectations in relation to material outsourcing to the public cloud

I am writing to all relevant firms to draw your attention to the Bank's existing supervisory expectations in relation to material outsourcing arrangements, including the use of public cloud, as they apply to Recognised Payment System Operators (RPSOs) and Specified Service Providers (SSPs).

The Bank's Financial Policy Committee (FPC) Q2 2021 record noted that since the start of 2020, financial institutions had accelerated plans to scale up their reliance on cloud service providers (CSPs). Although the Bank, FCA and PRA had recently strengthened their regulation of UK financial institutions' operational resilience, the increasing reliance on a small number of CSPs, and other critical third parties for vital services could increase financial stability risk in the absence of greater direct regulatory oversight of the resilience of the services they provide. The FPC also recognised that the use of the public cloud may bring benefits and opportunities, including potentially enhanced resilience compared to firms' on-premise IT infrastructure[1]. It may also lower operating costs, fuel innovation, and allow Financial Markets Infrastructure firms (FMIs) to adapt to the digital economy. However, there are associated risks that FMIs must manage; for example, ensuring that confidential, important or sensitive data outsourced to or shared with third parties is secure, and that outsourced services meet an appropriate standard of resilience.

RPSOs' and SSPs' reliance on third parties, in particular through outsourcing arrangements, is well established, and is already subject to existing guidelines set out in CPMI-IOSCO's Principles for Financial Market Infrastructure (PFMI), with which the Bank expects RPSOs to have regard[2]. These requirements also apply when RPSOs and SSPs wish to outsource to the public cloud. RPSOs and SSPs should also have due regard to the Bank's recently published policy on operational resilience[3] and considered any relevant international standards.

In particular, we expect RPSOs and SSPs to seek the Bank's non-objection if it is proposing a change to its business that could materially alter its business model or risk profile. This includes entering into, or significantly changing, any material outsourcing or sub-outsourcing arrangements. This also applies to arrangements with Cloud Service Providers (CSPs). We recommend that your firm engages with the Bank early to confirm whether a proposed change falls within the scope of these

[1] See, for example, Financial Stability Report July 2019 | Issue No. 45 (bankofengland.co.uk) and Financial Stability Report November 2018 | Issue No. 44 (bankofengland.co.uk).
[2] SSPs are expected to have regard to Annex F of the PFMIs
[3] See relevant links here: Bank of England policy on Operational Resilience of FMIs | Bank of England.

expectations and, if so, to discuss the information that the Bank will require to consider a non-objection in each case. You should submit the information sufficiently in advance of concluding any relevant contractual arrangement with the third party to allow time for the Bank to review your proposal in principle.

We also expect RPSOs and SSPs to notify the Bank, and seek the Bank's non-objection, when there could be a material change in its risk profile and that of the payments eco-system as a result of participants considering outsourcing their connectivity gateway or security solutions that are used to access your services to the public cloud. RPSOs may also need to introduce new or enhance existing control standards in its scheme rules to manage risks arising from such outsourcing arrangements to the payments eco-system, including through potentially requiring participants to secure the RPSO's agreement to any such move.

The Bank intends to consult on its proposed expectations and policies for FMIs on outsourcing in due course, with specific reference to cloud outsourcing.

Please refer to Annex I of the Bank's current expectations in relation to material outsourcing arrangements, and Annex II for the Bank's current expectations when there is a change in the risk profile of the payments eco-system should RPSOs and SSPs allow participants to host connectivity gateway and security solutions on the public cloud.

Yours sincerely

Simon Morley

Director, Financial Market Infrastructure Division

Annex I: Clarification of the Bank's supervisory expectations for material outsourcing arrangements, including with CSPs

We expect RPSOs and SSPs to pre-notify the Bank and seek the Bank's non-objection when proposing a change to their business model that could materially alter their business model or risk profile. This includes entering into, or significantly changing, material outsourcing arrangements with CSPs. Material outsourcing includes outsourcing or sub-outsourcing of critical operations or important business services (once identified) as set out in the Bank's operational resilience policy, which will come into force in March 2022. The Bank expects RPSOs and SSPs to make these notifications before entering into, or amending, their outsourcing arrangements.

When a material outsourcing arrangement includes critical operations or important business services, RPSOs and SSPs remain responsible and accountable for the outsourced service(s) and are expected to have a robust contractual framework and effective controls to mitigate potentially increased risks. Specifically, the Bank expects RPSOs and SSPs to comply with guidelines set out in PFMI Principle 17 – Operational Risk and demonstrate how they will achieve the following outcomes through the proposed outsourcing arrangement. In our view, this includes the following:

a) RPSOs and SSPs remain responsible for the delivery of their critical operations or important business services and exercising appropriate oversight of third party service providers. For example, the RPSO or SSP should maintain sufficient skills and capabilities for managing the risks arising from outsourcing arrangements, perform appropriate and proportionate due diligence on potential service providers and fully assess the risk of all outsourcing arrangements, including any sub-outsourcing arrangements.

b) RPSOs and SSPs have robust risk management procedures in place that ensure appropriate safeguards to manage and monitor relevant risks, including data security, service availability and data integrity; provisions for rights of access, audit and information rights (both for themselves, the Bank as its supervisor, and persons appointed on their behalf); and early termination and exit arrangements.

c) RPSOs and SSPs will continue to deliver their critical operations or important business services in a robust, resilient and secure manner. For example, when outsourcing to the public cloud, the contractual arrangements should highlight the respective roles and responsibilities of the RPSO / SSP and third party service providers in all areas, including data security, system configuration, data classification, implementing controls, and ensuring compliance with legal and regulatory requirements. RPSOs and SSPs must have considered the legal and security risks if data storage and/or processing is located in another country, and have taken appropriate steps to mitigate such risks.

d) The use of outsourced service providers must not undermine an RPSO's or SSP's ability to recover and meet its operational resilience objectives. For example, the RPSO's and SSP's business continuity plans should consider their ability to deliver any critical operations or important business services provided or supported by third parties in line with the RPSO's / SSP's impact tolerance in the event of third party disruption. An RPSO's and SSP's business continuity plans should be tested under extreme but plausible scenarios of disruption.

e) RPSOs and SSPs should have a documented exit strategy to transition the delivery of critical operations or important business services to a new service provider or in-house, or take any other necessary measures to ensure appropriate continuity of service, in the event of a failure or prolonged disruption of the third party service provider. RPSOs and SSPs should test the exit strategy and be able to demonstrate transition of the critical operations or important business services to a new provider or to itself without service interruption.

Annex II: Clarification of the Bank's supervisory expectations when there is a material change in the risk profile of RPSOs and SSPs arising from participants hosting FMI connectivity gateway and security solutions on the public cloud

We expect RPSOs and SSPs to notify the Bank and seek the Bank's non-objection when there is a material change in their risk profile, and that of the payments eco-system. This may include allowing participants to outsource connectivity gateway and security solutions to the public cloud.

The Bank expects RPSOs and SSPs to have identified and be appropriately managing the risks arising from participants' outsourcing arrangements. RPSOs are expected to manage the increase in complexity in the eco-system stemming from CSPs hosting participants' FMI connectivity gateway and security solutions. RPSOs may also change its scheme rules to introduce new control standards to manage risks arising from such outsourcing arrangements to the payments eco-system.

Specifically, the Bank expects RPSOs and SSP to comply with guidelines set out in PFMI Principle 3 – Framework for comprehensive management of risks and Principle 18 – Access and participation requirements, and will seek evidence that RPSOs and SSPs are able to demonstrate effective governance, and that they are able to manage their eco-system to set, monitor and enforce standards, including those relating to information security and operational resilience. In our view, this includes the following:

a) RPSOs' scheme rules should be adequate to manage the change to their risk profile arising from participants outsourcing connectivity and security solutions to the public cloud, and ensure the safe, effective and resilient operation of the eco-system. The standards set out by RPSOs' scheme rules may set out the expectations that participants must meet to manage associated technology risks, and requirements for participants to test the resiliency of the solution outsourced to third parties.

b) RPSOs have established appropriate and proportionate assurance and compliance procedures to ensure participants comply with the scheme rules.

c) RPSOs and SSPs have sufficient skills and capabilities to identify, assess and manage the changes to their risk profile arising from participants outsourcing connectivity and security solutions to the public cloud, including any material change in the risk profile of the payments eco-system to ensure that it remains safe and resilient.

d) RPSOs and SSPs should monitor the risk of a concentration of participants outsourcing connectivity gateway and security solutions to a small number of CSPs, and have assessed the risk of a prolonged outage at a CSP affecting multiple participants simultaneously, and thereby impacting the smooth functioning of the payments eco-system.