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 Central Counterparties (CCPs).

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.

CCPs' reliance on third parties, in particular through outsourcing arrangements, is well established, and is already subject to existing regulatory requirements and CPMI-IOSCO Principles for Financial Markets Infrastructure (PFMI), with which the Bank expects CCPs to have regard. This includes the outsourcing requirements set out in Article 35(1) of the onshored Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (UK EMIR). This requirement applies when CCPs wish to outsource the delivery of its activities linked to risk management, or parts thereof to the public cloud. CCPs should also have due regard to the Bank's recently published policy on operational resilience[2] and consider any relevant international standards.

In particular, I wish to remind you to notify the Bank before entering into, or significantly changing, any material outsourcing, or sub-outsourcing arrangements, including arrangements with CSPs, so

[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] See relevant links here: Bank of England policy on Operational Resilience of FMIs | Bank of England.

that we can assess compliance of the plans with the relevant regulation. We recommend that you engage with the Bank early to confirm, if necessary, whether a proposed change falls within the scope of these requirements and, if so, to discuss the information that the Bank will require to provide our approval in each case. You should submit the information sufficiently in advance of concluding any relevant contractual arrangement with the third party to allow the Bank to review your proposal in principle.

We also expect CCPs to notify the Bank, and seek the Bank's non-objection, of any substantive changes that could affect the compliance with the conditions for authorisation. This includes any material change in your risk profile and that of the CCPs' clearing system as a result of participants considering outsourcing their connectivity gateway and security solutions that are used to access your services to the public cloud. CCPs may also need to introduce new or enhance existing control standards and rules to manage risks arising from such outsourcing arrangements to the CCPs and its clearing eco-system, including through potentially requiring participants to secure CCPs' 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 the use of Cloud.

Please refer to Annex I for clarification 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 CCPs and the clearing eco-system should CCPs 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 CCPs to notify the Bank and seek the Bank's approval when entering into, or significantly changing, material outsourcing arrangements or sub-outsourcing of activities linked to risk management or parts thereof as defined in UK EMIR. The Bank expects CCPs to make these notifications before entering into, or amending, the outsourcing arrangement. When a material outsourcing arrangement includes critical functions or important business services (once identified) as set out in the Bank's operational resilience policy, which will come into force in March 2022, we expect CCPs to also pre-notify the Bank and seek the Bank's non-objection when entering into, or significantly changing, material outsourcing arrangements with CSPs.

A CCP remains responsible and accountable for the outsourced service(s) and is required to have a robust contractual framework and effective controls to mitigate potentially increased risks. Specifically, the Bank expects a CCP to comply with the requirements set out in UK EMIR Article 35 and guidelines set out in PFMI Principle 17 – Operational Risk. In our view, this includes the following:

a) Where a CCP outsources operational functions, services or activities, it shall remain fully responsible for discharging all of its obligation under UK EMIR regulation. For example, the CCP maintains sufficient skills and capabilities for managing the risks arising from outsourcing arrangements, performs appropriate and proportionate due diligence on potential service providers and assesses the risks of every outsourcing arrangement, including any sub-outsourcing arrangements. This is consistent with UK EMIR Article 35(1)(g).

b) The CCP has 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 (for itself, the Bank as its supervisor, and persons appointed on their behalf) and early termination; and exit arrangements. This is consistent with UK EMIR Article 35(1)(e), 35(1)(f) and 35(1)(j).

c) The CCP continues to deliver its critical functions or important business services in a robust, resilient and secure manner. For example, when outsourcing to the public Cloud, the contractual arrangement should highlight the respective roles and responsibilities of the CCP and third party service providers in all areas, including data security, system configuration, data classification, implementing controls and ensuring compliance with legal or regulatory requirements. The CCP 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. This is consistent with UK EMIR Article 35(2) and (3)

d) The use of outsourced service providers must not undermine a CCP's ability to recover and meet its operational resilience objectives, including requirements set out in Articles 17-23 of the onshored regulatory technical standards 153/2013 (UK EMIR RTS). For example, the CCP's business continuity plans must consider its ability to deliver any critical functions or important business services provided or supported by third parties in line with the CCP's impact tolerance in the event of third party disruption. A CCP's business continuity plans should be tested under extreme but plausible scenarios.

e) The CCP's business continuity or disaster recovery plans should include a documented exit strategy to transition the delivery of critical functions or important business services to a new service provider or in-house, or take any viable measures to ensure appropriate continuity of service, in the event of a failure or prolonged disruption of the third party service provider. The CCP must test the exit strategy and be able to demonstrate transition of the critical functions or important business

service to a new provider or to itself without service interruption. This is consistent with UK EMIR RTS Articles 19 and 20.

Annex II: Clarification of the Bank's supervisory expectations when there is a material change in the risk profile of CCPs

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

The Bank expects CCPs to have identified and appropriately manage the risks posed by key participants. CCPs are expected to manage the increase in complexity in the eco-system stemming from CSPs hosting participants' CCP connectivity gateway and security solutions, and comply with risk management requirements set out in UK EMIR RTS Article 4(1). CCPs should also have due regard to the guidelines set out in PFMI Principle 3 – Framework for comprehensive management of risks, and Principle 18 – Access and participation requirements. Specifically, the Bank will require CCPs to demonstrate effective governance, and that they are able to manage their eco-system to set, monitor and enforce standards, including those relating to security and resilience. In our view, this includes the following:

a) CCPs' participation requirements shall ensure that clearing members have sufficient financial resources and operational capacity to meet the obligations arising from participation in a CCP. These may include risks arising from participants outsourcing connectivity and security solutions to the public Cloud, and ensure the safe, effective and resilient operation of the eco-system. This is consistent with the requirements of UK EMIR Article 37(1). For example, CCPs' participation requirements may set specific standards that participants must meet on IT security and requirements for participants to test the resiliency of the solution outsourced to third parties.

b) CCPs have established appropriate and proportionate assurance and compliance procedures to ensure participants comply with its participation requirements. This is consistent with the requirements of UK EMIR Article 37(2)

c) CCPs have the necessary skills and capabilities to identify, assess and manage risks arising from participants outsourcing connectivity and security solutions to the public cloud, including any material change in the risk profile of the CCP's eco-system to ensure that it remains safe and resilient. This is consistent with requirements set out in UK EMIR RTS Article 4(6).

d) CCPs monitor the risk of a concentration of participants outsourcing connectivity and security solutions to the public Cloud, and has assessed the risk of a prolonged outage at a CSP affecting multiple participants simultaneously, and thereby impacting the smooth functioning of the CCP's eco-system. This is consistent with requirements set out in UK EMIR Article 37(3).