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 Securities Depositories (CSDs).

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.

CSDs reliance on third parties, in particular through outsourcing arrangements, is well established, and is already subject to existing regulatory requirements and CPMI-IOSCO's Principles for Financial Markets Infrastructure (PFMI), with which the Bank expects CSDs to have regard. This includes the authorisation requirement set out in Article 19 of the onshored Regulation (EU) No 909/2014 of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories (UK CSDR), where the outsourcing relates to the delivery of core services as defined in Section A of the Annex. This requirement applies when CSDs wish to outsource the delivery of its core services or parts thereof to the public cloud. CSDs should also have due regard to the Bank's recently published policy on operational resilience[2] and consider any relevant international standards.

[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.

In particular, I wish to remind you that the requirement to submit an application for authorisation for outsourcing in accordance with Article 19(1) of the UK CSDR before entering into, or significantly changing, any material outsourcing, or sub-outsourcing, also applies to arrangements with CSPs. 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 authorisation 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 CSDs 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 its risk profile and that of the CSDs' securities 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. CSDs may also need to introduce new or enhance existing control standards and operational requirements to manage risks arising from such outsourcing arrangements to the CSDs securities settlement eco-system, including through potentially requiring participants to secure CSD'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 the use of cloud.

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 CSDs and the securities settlement system should CSDs 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 a CSD to notify the Bank and seek the Bank's authorisation when entering into, or significantly changing, material outsourcing arrangements or sub-outsourcing of its core services or parts thereof as defined in UK CSDR. The Bank expects CSDs to make these notifications before entering into, or amending, the outsourcing arrangement. When a material outsourcing arrangement includes 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, we expect CSDs to also pre-notify the Bank and seek the Bank's non-objection when entering into, or significantly changing, material outsourcing arrangements with CSPs.

CSDs remain 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 CSD to comply with the requirements set out in UK CSDR Article 30 and guidelines set out in PFMI Principle 17 – Operational Risk. In our view, this includes the following:

a) The CSD remains responsible for the delivery of its critical operations or important business services and is able to exercise appropriate oversight of third party service providers. For example, the FMI 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.

b) The CSD 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 (both for itself, the Bank as its supervisor, and persons appointed on their behalf) and early termination; and exit arrangements.

c) The CSD continues to deliver its critical operations 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 CSD 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 CSD 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 a CSD's ability to recover and meet its operational resilience objectives, including requirements set out in Articles 76-80 of the onshored regulatory technical standards 2017/392 (UK CSDR RTS). For example, the CSD's business continuity plans must consider its ability to deliver any critical operations or important business services provided or supported by third parties in line with the CSD's impact tolerance in the event of third party disruption. A CSD's business continuity plans should be tested under extreme but plausible scenarios.

e) The CSD's business continuity or disaster recovery plans should include 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 viable measures to ensure appropriate continuity of service, in the event of a failure or prolonged disruption of the third party service provider. The CSD must test the exit strategy and be able to demonstrate transition of the critical operations or important business service to a new provider or to itself without service interruption, including requirements set out in UK CSDR RTS Article 78-79.

Annex II: Clarification of the Bank's supervisory expectations when there is a material change in the risk profile arising from substantive changes affecting the compliance with the conditions for authorisation.

We expect a CSD 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 securities settlement system. This may include allowing participants to outsource connectivity gateway and security solutions to the public cloud to access the securities settlement system.

The Bank expects CSDs to have identified and appropriately managing the risks posed by key participants. CSDs are expected to manage the increase in complexity in the eco-system stemming from CSPs hosting participants' CSD connectivity gateway and security solutions, and comply with risk monitoring requirements set out in UK CSDR RTS Article 47, 48 and 49. CSDs 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 CSDs 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) CSDs shall have clear and transparent criteria, methodologies and standards in order that key participants meet the operational requirements. This includes managing the risks arising from participants outsourcing connectivity and security solutions to the public cloud, and that the operational risks posed by key participants are managed to ensure a safe and resilient operation of the eco-system. This is consistent with requirements set out in UK CSDR RTS Article 67(3). For example, CSD 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) CSDs have established appropriate and proportionate assurance and compliance procedures, and on an ongoing basis to identify, monitor and manage the operational risks that it faces from key participants. This is consistent with requirements set out in UK CSDR RTS Article 67(4).

c) CSDs have sufficient 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 CSD's eco-system to ensure that it remains safe and resilient. This is consistent with requirements set out in UK CSDR RTS Article 70(2).

d) CSDs 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 CSD's eco-system. This is consistent with the requirement set out in UK CSDR Article 42 require CSDs to adopt a sound risk management framework for comprehensively managing legal, business, operational and other direct or indirect risks.