Bank of England

Review Questions

Limit breaches

Key judgement on limit breaches: does the entrant have a plausible approach to abide by our limits, including through having the controls and processes in place to monitor limits utilisation, act if limits are approached, and rectify and report any limits breaches?

On early warning

1. What systems or mechanisms are in place to provide early warnings before a limit is breached?

2. How do these mechanisms trigger alerts, and what actions can be taken before the breach occurs?

3. Are there predefined thresholds or escalation points that indicate when a limit is approaching? If so, how they are set and adjusted over time?

Detecting breaches

4. How does your system track and monitor limit breaches in real time? Does this approach differ by asset class?

5. What metrics do you use to determine if a limit has been breached?

6. How quickly can the technology identify a limit breach?

7. What automated controls and/or manual processes are in place to detect breaches promptly?

Preventing breaches

8. How will breaches of limits be prevented in your system? What controls do you have in place to ensure that breaches do not occur?

Responding to breaches

9. What steps does your firm take when a limit is breached?

10. How would you report and respond to any breaches internally and to regulators?

Cyber controls

Key judgement: does the entrant have in place a minimal cyber security risk management approach, and does it have a plausible way of mitigating cyber contagion risk?

On maturity assessment

1. Has the firm developed a maturity assessment model to assess and improve your cybersecurity capabilities? If so, please explain which maturity model you are using, and explain how it assesses your current maturity level against your target environment. Describe any key areas you have identified for improvement.

Detecting and preventing cyber attack

2. Does the firm place any reliance on your participants' or third parties' cyber security measures in managing cyber contagion risks?

3. What are the entry points into the firm's system? Do these change based on the stage of the DLT process? How will it detect and protect threats against each of them?

4. Under its business/operating model, what key cybersecurity risks has the firm identified and what relevant controls has the firm developed to mitigate the impact/probably of those risks crystallising?

Response and recovery

5. What are the firm's key cyber response and recovery capabilities and what gaps have you identified? What type of cyber scenarios, if considered, are identified and tested as part of your BCP/ITDR?

6. In the event of a successful cyber-attack (e.g. data integrity/ransomware) severely impacting its ICT infrastructure:
   - How will the firm continue to securely communicate to participants/stakeholders?
   - What are the firm's key controls to protect participant data (or register of ownership) and assets? How would the effectiveness of these controls be compromised if the firm is subject to a successful cyberattack, e.g. data integrity or ransomware attack?
   - What controls does the firm have to mitigate the risk of contagion to its participants and connected third parties?

Asset loss questions

Key judgement: do the ledger, smart contracts, and central controls work collectively in a way that allows for assets to be plausibly recovered and reconciled to participants in the event of data corruption or theft?

Ledger appropriateness

1. Do the ledger(s) utilised meet the business needs of the firm?

2. Are the instruction stages that directly impact data integrity (i.e., the ordering stage and the validation stage) known to function reliably in the ledger(s) utilised by the firm?

Central controls (ledger)

3. What central controls does the firm have over the ledger system?

4. Can the assets be recovered from a backup under central control of the DSD?

5. Are central controls required at the smart contract level to assist in recovery and afford control to the DSD, and if so, are these controls implemented?

Central controls (smart contracts)

6. Can the firm reestablish ownership of digital assets in the event of a smart contract failure?

7. Does the smart contract used afford recovery controls for the digital assets?

8. Does the smart contract ensure clarity on the legal claim to the security?

9. Are central controls required at the authentication mechanism level to assist in recovery and afford control to the DSD, and are these controls implemented?

Central controls (authentication mechanisms)

10. Can you reestablish ownership of digital assets in the event of a failure in the authentication mechanism utilised (e.g., multi-party computation)?

11. Does the authentication mechanism utilised ensure clarity on the legal claim to the security?

Asset reconciliation and recovery

12. Are the digital assets designed in a way that enables rights of ownership to be enforced, should there be a claim (under the laws of the UK)?

13. Can the firm protect the custody of the assets, communications of instructions, ledger access, and technology in place to store backup records from potential data corruption or theft? How?

Wind-down

Key judgement: does the entrant have a wind-down plan that can plausibly facilitate the protection and return of client assets in a wind-down scenario – both financial and operational?

Preparations for wind-down

1. What are the key (operational and financial) triggers that would initiate your wind-down plan?

2. What are the stressed scenarios underpinning your wind-down plan, covering both operational and financial failures (including relating to an extreme but plausible cyber attack)? And what is your rationale for choosing these scenarios?

3. How frequently will you test and review the feasibility of your wind-down plan?

Wind-down plan

4. What steps would you take to ensure an orderly exit from the DSS?

5. How would you communicate the wind-down to participants and regulators?

6. How would you ensure that the transfer of assets or settlement are completed during a wind-down?

Funding and dependencies

7. How do you ensure that funding is available to cover operational costs until all obligations have been met?

8. Have you mapped dependencies on third parties and assessed how they would be managed in a wind-down?