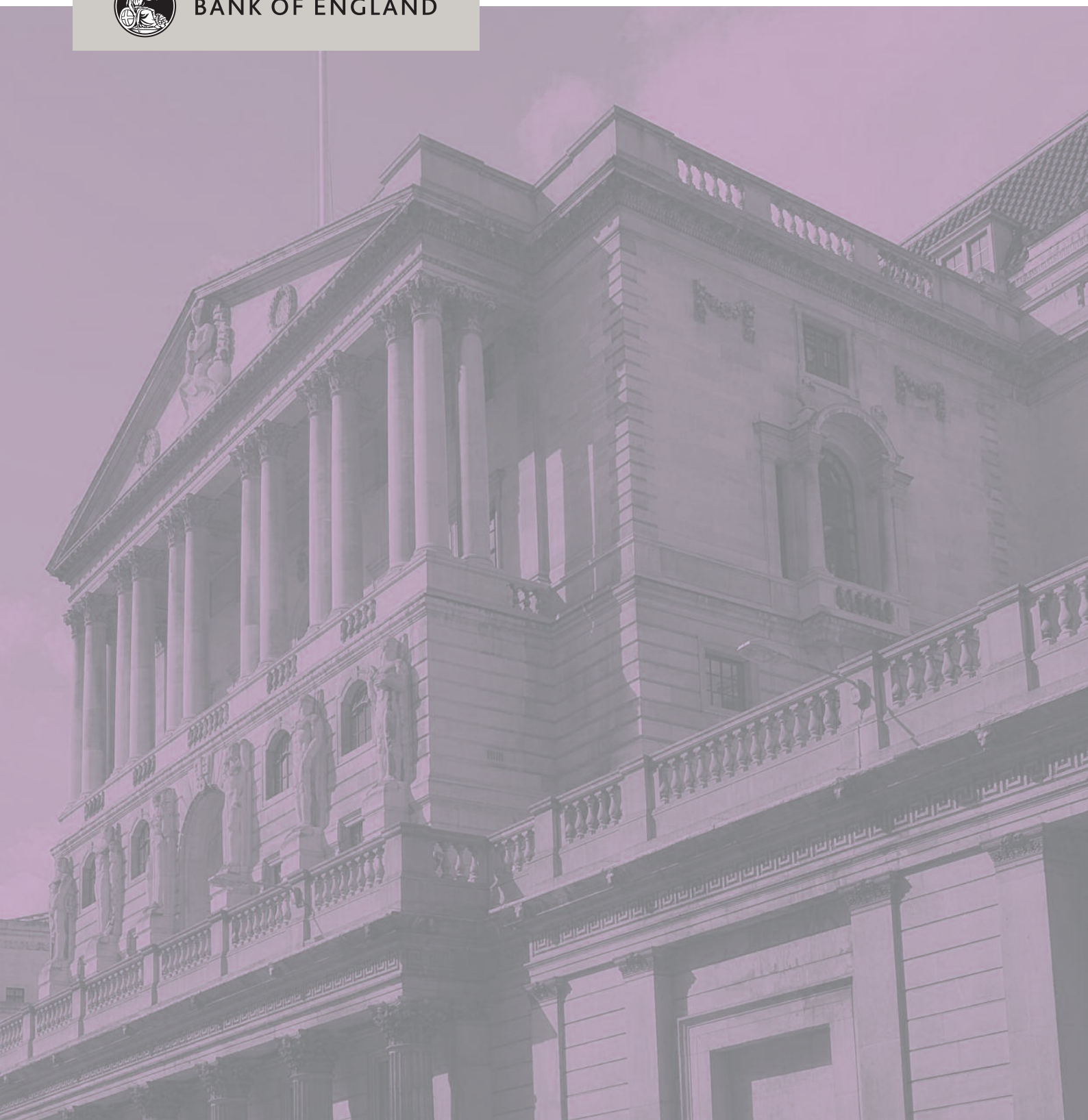
Feedback to Consultation Responses

Consultation on a new rule for Central Counterparties relating to incident reporting

May 2018

BANK OF ENGLAND



BANK OF ENGLAND

Feedback to Consultation Responses

Consultation on a new rule for Central Counterparties relating to incident reporting

May 2018

The Bank of England provides feedback to responses received to the consultation paper issued in February 2018 on a new rule for Central Counterparties relating to incident reporting.

Copies of this paper are available to download from the Bank's website at www.bankofengland.co.uk.

Overview

The Bank of England (the Bank) issued a consultation paper(1) in February 2018 (February CP) on a new rule it is proposing to make relating to incident reporting for UK central counterparties (CCPs). The proposed new rule formalises the requirement for CCPs to notify the Bank of certain incidents having an impact on their information technology systems.

Following the consultation and consideration of responses received, the Bank has decided to proceed with the rule as proposed. The rule is effective and binding on CCPs from 7 May 2018.

Consultation responses and Bank feedback

The Bank received three responses from a range of financial market infrastructure (FMI) firms to the February CP on the new rule for CCPs relating to incident reporting. Respondents were broadly supportive of the proposed rule. Respondents raised a number of points in relation to the Bank's proposed approach and the drafting of the rule. These are discussed below by topic along with the Bank's response.

Meaning of 'significant impact'

The proposed rule requires a CCP to give the Bank of England written notice of an incident having a significant impact on the continuity of services it provides. Several respondents provided feedback on the use of the term 'significant' in this context, although there was a divergence of views as regards whether this should be defined or remain as currently drafted.

The Bank considered whether it would be beneficial to define the term 'significant', for instance, by reference to specified *ex ante* thresholds for reporting under this rule. However the Bank concluded that CCPs would be better placed to determine the significance of impact of an incident on the continuity of services they provide, given the broad scope of incidents that may occur and wide ranging impacts these could have, and has therefore chosen not to define the term.

Some respondents additionally noted that appropriate incident reporting and information sharing thresholds have been discussed and agreed with their supervisor. As stated in the February CP, the Bank expects FMIs, including CCPs, to continue to adhere to current supervisory practices, and the proposed rule is without prejudice to such practices.

Types of incidents

The February CP provided a definition of a reportable incident within the context of the proposed rule. The responses received indicated that firms wanted further clarification of what types of incidents would be reportable.

Under the proposed rule, a reportable incident is one that has an actual adverse effect on the security of information technology systems (as defined in the proposed rule). This means that the cause of the incident is not the determinative factor in whether an incident needs to be reported, as the rule relates to the impact of the incident. The rule would therefore include cyber incidents, non-cyber incidents, and incidents that are both cyber and non-cyber — ie any type of incident that has the relevant adverse effect.

An example of a cyber incident that affects the security of information technology systems may be a malware infiltration via mobile devices or an employee clicking on a malicious link in an email leading to malware infection. An example of a non-cyber incident that affects the security of information technology systems may be a flood that damages servers or power outage at a data centre. An example of an incident that is both cyber and non-cyber may be a physical theft of a server, followed by the sale or harvesting of the data held on that server.

Reporting of incidents

Some respondents sought further clarification on the expected timescales for providing notifications to the Bank and the ways in which such notice may be provided.

The proposed rule requires CCPs to notify the Bank of relevant incidents as soon as reasonably practicable, which may include intraday reporting. CCPs, and FMIs more generally, provide essential services that are vital to the stability of the financial system. The timeliness of an FMI's intraday functions is critical in providing services. Additionally, the Bank has existing supervisory expectations of timely notification of incidents by FMIs. We believe this is still appropriate and FMIs should continue to meet such expectations.

One respondent noted that impact reporting may evolve during an incident, because the impact level could change as further details and understanding of an incident are discovered. The Bank recognises the potentially evolving nature of incidents, and would expect to receive additional reports as the incident and/or impact thereof evolves.

The proposed rule requires incident reporting to the Bank via written notice (for example, through email to appropriate supervisory contacts). This is without prejudice to existing practices as may be appropriate in each case such as, for example, separately contacting the FMI's supervisors by telephone.

(1) www.bankofengland.co.uk/paper/2018/new-rule-for-central-counterparties-relating-to-incident-reporting.

Other feedback

Respondents also provided feedback on the Bank's supervisory approach relating to incident reporting more generally. Some FMIs suggested the Bank could use incident reporting across firms to compare and share trends with affected and interested parties in the industry. As outlined in the Bank's FMI Annual Report,(2) the Bank regularly undertakes thematic (cross-FMI) work and shares the findings; this would also apply to work undertaken in relation to operational resilience.

Conclusion

The Bank will proceed with the rule as proposed in the February CP.

The full wording of the rule is available on the Bank website at www.bankofengland.co.uk/financial-stability/financial-market-infrastructure-supervision, which will be effective and binding on CCPs from 7 May 2018.

(2) www.bankofengland.co.uk/news/2018/february/supervision-of-financial-market-infrastructures-annual-report-2018.