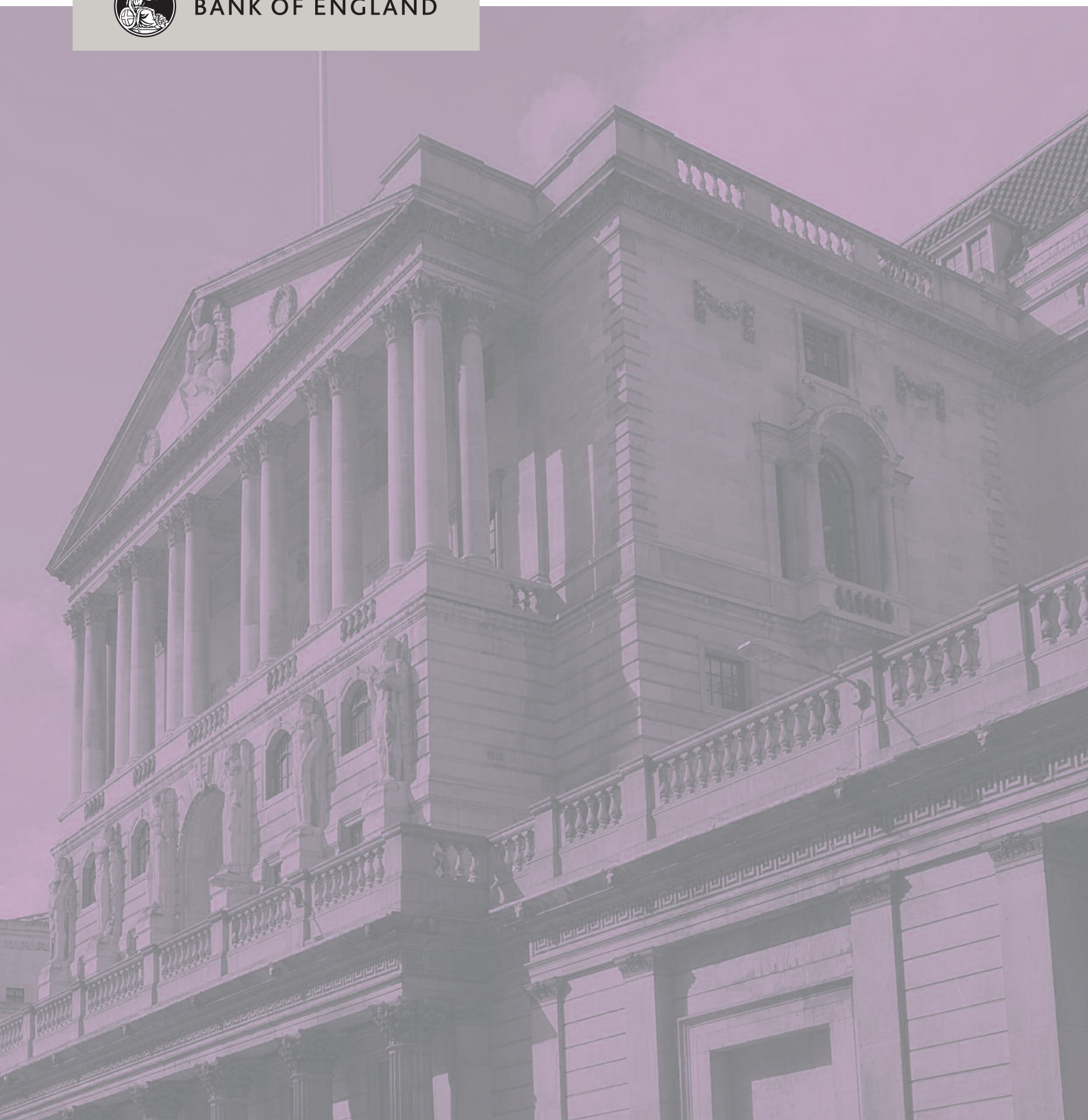
Consultation Paper

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

February 2018

BANK OF ENGLAND



BANK OF ENGLAND

Consultation Paper

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

February 2018

The Bank of England invites comments on this Consultation Paper. Comments should reach the Bank by 3 April 2018.

Comments may be sent by email to FMIFeedback@bankofengland.co.uk.

Alternatively, please send comments in writing to:
FMI Feedback
Financial Market Infrastructure Directorate
Bank of England
20 Moorgate
London EC2R 6DA

The Bank may make responses to this consultation public unless the respondent requests otherwise. A standard confidentiality statement in an email message will not be regarded as a request for non-disclosure. If the Bank receives a request under the Freedom of Information Act 2000, the Bank may consult respondents who had requested confidentiality. Any decision the Bank makes not to disclose a response is reviewable by the Information Commissioner and the Information Rights Tribunal.

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

Overview

The Bank of England (the Bank), as the competent authority with responsibility for the supervision of UK central counterparties (CCPs), receives notifications from CCPs of incidents relating to their information technology systems.(1) This is important in allowing the Bank to discharge its supervisory mandate and in pursuit of its mission to promote monetary and financial stability.

Currently the Bank receives these notifications in accordance with a supervisory expectation. This consultation seeks feedback on a new rule the Bank is proposing to make relating to incident reporting, which will formalise the requirement for CCPs to notify the Bank of certain incidents having an impact on their information technology systems.

The proposed rule set out in this Consultation Paper would support the UK Government's approach to the implementation of the EU Network and Information Systems Directive. It would be made using the Bank's powers under the Financial Services and Markets Act 2000 (FSMA). As a result, the relevant requirements are those set out in s293 of FSMA.

Background

The Bank currently has a supervisory expectation that CCPs promptly notify the Bank of any operational incidents as soon as reasonably practicable, including any incidents that affect the security of their information technology systems. While this is not a formal rule at present, in practice, it means CCPs contact the Bank in the event of an incident and keep the Bank updated at regular intervals until the incident is resolved. Other UK financial market infrastructures (FMIs) follow a similar approach.

The Bank is proposing to introduce a new rule for CCPs which will formalise some aspects of the current supervisory expectation in relation to the reporting of operational incidents.

The importance of robust network and information security requirements has been recognised by the EU and on 6 July 2016 Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (the Directive) was adopted.

The Directive covers operators of essential services across thirteen sectors including FMIs. Of the FMIs supervised by the Bank, only CCPs are in-scope of the Directive. A key aspect of the Directive is ensuring operators of essential services are required to take appropriate and proportionate security measures to manage risks to their network and information systems, and notify incidents having a significant impact on the continuity of the services they provide to the relevant authority. Member states have until 9 May 2018 to implement the Directive into domestic legislation.

The UK Government issued a public consultation in August 2017 setting out its proposed approach towards implementing the Directive in the United Kingdom.(2) In relation to the banking and FMI sectors, the consultation stated:

> 'In line with Article 1(7) of the Directive, the banking and financial market infrastructures sectors within scope of the Directive will be exempt from aspects of the Directive where provisions at least equivalent to those specified in the Directive will already exist by the time the Directive comes into force. Firms and financial market infrastructure within these sectors must continue to adhere to requirements and standards as set by the Bank of England and/or the Financial Conduct Authority.'

In line with the Government's proposed approach with respect to FMIs in relation to the Directive, the Bank is proposing to introduce a new rule for CCPs which formalises some aspects of the current supervisory expectation in relation to operational incident reporting. The rule is expected to come into effect by 9 May 2018.

The Bank encourages other FMIs to also follow this rule, noting it is not a binding requirement on them.

Purpose of the rule and financial stability objective

Incident reporting allows the Bank to receive critical information about disruptions to the continuity of essential financial services, and to share critical information with the National Cyber Security Centre (NCSC; the United Kingdom's technical authority on cyber security issues) subject to permission from the impacted organisation. The NCSC also acts at the single point of contact for incidents at other operators of essential services. The Bank considers knowledge of incidents to be an important part of developing a shared understanding of risks, and a vital part of reducing the overall threat to the FMI sector and the financial sector as a whole.

CCPs constitute part of the United Kingdom's critical national infrastructure due to their central role in clearing and settlement. If CCPs were unable to perform this function, trading on exchanges and in over-the-counter markets would be disrupted. This could have a detrimental effect on market

(1) The definition for 'information technology systems' can be found at the end of this paper.
(2) www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive.

liquidity, market confidence and financial stability. Over the longer term this could have a negative impact on London's reputation as a financial centre.

Incident reporting

The proposed rule is intended to supplement existing practices by requiring a CCP to report certain incidents to the Bank.

The notification requirement would cover any incident, including a physical event, affecting the security of a CCP's information technology systems that had a significant impact on continuity of services provided. The inclusion of physical events is common to most international standards; for example the PFMI covers Physical and Information security and ISO 270001, the National Institute of Standards and Technology Framework and the Cloud Controls Matrix cover cyber and information technology systems.

The proposed rule requires a CCP to report an incident as soon as reasonably practicable after it becomes aware of the incident. A CCP is also required (either concurrently or as soon as reasonably practicable after providing notification of an incident) to provide information which would allow the Bank to determine any impact of the incident, such as financial, operational or legal.

Defining an incident

A reportable incident within the context of this rule, and in line with the Directive, is defined as:

- Any event that has a significant impact on the continuity of services CCPs provide;
- One that has an actual adverse effect on the security of information technology systems used in the provision of essential services; and
- Where the 'security of information technology systems' means the ability of information technology systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those information technology systems.

The Bank considers there is an impact on continuity where there is a loss, reduction or impairment of an essential service.

The Bank expects FMIs, including CCPs, to continue the current supervisory practice of notifying incidents and/or providing information in relation to such incidents as agreed

Proposed rule

[RCH 4] Notification of incidents

4.1 A recognised central counterparty must give the Bank of England written notice of an incident having a significant impact on the continuity of services it provides.

4.2 A recognised central counterparty must give such notice as soon as reasonably practicable after it becomes aware of the incident.

4.3 Without prejudice to the generality of paragraph [4.1], a recognised central counterparty must provide such information in connection with a notification (either concurrently or as soon as reasonably practicable thereafter) as will enable the Bank of England to determine the impact of the incident.

4.4 This rule is without prejudice to any other power of the Bank of England to require, or ability of the Bank of England to request, notifications or information from recognised central counterparties.

4.5 In this rule, in respect of a recognised central counterparty:

(a) 'incident' means any event having an actual adverse effect on the security of information technology systems;

(b) 'information technology system' includes a 'network and information system' as such term is defined in Article 4(1) of Directive 2016/1148/EC; and

(c) 'security of information technology systems' means the ability of information technology systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those information technology systems.

with their supervisor. This could include voluntary reporting of incidents that do not meet the above thresholds, such as:

- Incidents where operators have to take action to maintain supply, provision, confidentiality or integrity of the service; or

- Incidents where software/intrusions are found that could potentially disrupt, or allow to be disrupted, the supply, provision, confidentially or integrity of the service.

Cost-benefit analysis

Section 138J(2)(a) of FSMA, as applied to the Bank by virtue of paragraph 10 of Schedule 17A to FSMA, requires the Bank to publish a cost-benefit analysis when proposing draft rules. Section 138L(3) of FSMA provides that this requirement does not apply where the Bank considers there will be no increase in costs or that any increase in costs will be of minimal significance.

Having assessed the proposed rule and having regard to existing practices whereby incident reporting by CCPs is already undertaken today in accordance with existing supervisory expectations, the Bank considers any costs imposed as a result of the proposed rule will be of minimal significance.

Questions

(1) Do you agree with the approach proposed in this rule?

(2) Do you have any comments on the Bank's drafting of the rule?