

Operational resilience: operational incident and outsourcing and third-party reporting for financial market infrastructures

Consultation paper

Published on 13 December 2024

Content

Privacy statement

Consent to publication

1: Overview

Background

Structure of the CP

Cost benefit analysis

Implementation

Responses and next steps

2: Operational incident reporting

Operational incident

Reporting thresholds

Phased approach to reporting operational incidents

Initial operational incident report

Intermediate operational incident report

Final operational incident report

Format of operational incident reports

Operational incident data

Statutory obligations

3: Outsourcing and third-party reporting

Material third-party arrangements

Notifications

Register

Information to submit to the Bank

Statutory obligations

4: Have regards analysis

Appendices

The Bank of England is consulting on operational incident and outsourcing and third-party reporting (IOREP) rules for financial market infrastructures (FMIs). These rules set a framework for high-quality and consistent reporting of the operational incidents and third-party arrangements that may have the greatest impact on financial stability. They aim to support the operational resilience of the UK financial sector and the Bank's ability to monitor and manage potential risks. The Bank is following a joint approach with the Prudential Regulation Authority and Financial Conduct Authority, who are consulting in parallel. The Bank's consultation is open until 13 March 2025, and responses should be sent to: ✉ FMI-IOREP-CP@bankofengland.co.uk.

Privacy statement

By responding to this consultation, you provide personal data to the Bank of England. This may include your name, contact details (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself.

The response will be assessed to inform our work as a regulator and central bank, both in the public interest and in the exercise of our official authority. We may use your details to contact you to clarify any aspects of your response.

The consultation paper will explain if responses will be shared with other organisations (for example, the Financial Conduct Authority). If this is the case, the other organisation will also review the responses and may also contact you to clarify aspects of your response. We will retain all responses for the period that is relevant to supporting ongoing regulatory policy developments and reviews. However, all personal data will be redacted from the responses within five years of receipt. To find out more about how we deal with your personal data, your rights, or to get in touch please visit [Privacy and the Bank of England](#).

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure to other parties in accordance with access to information regimes including under the Freedom of Information Act 2000 or data protection legislation, or as otherwise required by law or in discharge of the Bank's functions.

Please indicate if you regard all, or some of, the information you provide as confidential. If the Bank receives a request for disclosure of this information, we will take your indication(s) into account but cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system on emails will not, of itself, be regarded as binding on the Bank.

Responses are requested by 13 March 2025.

Please address any comments or enquiries by email to: ✉ FMI-IOREP-CP@bankofengland.co.uk.

Consent to publication

The Bank publishes a list of respondents to its consultations, where respondents have consented to such publication.

When you respond to this consultation paper, please tell us in your response if you agree to the publication of your name, or the name of the organisation you are responding on behalf of, in the Bank's feedback response to this consultation.

Please make it clear if you are responding as an individual or on behalf of an organisation.

Where your name comprises 'personal data' within the meaning of data protection law, please see the Bank's Privacy Notice above, about how your personal data will be processed.

Please note that you do not have to give your consent to the publication of your name. If you do not give consent to your name being published in the Bank's feedback response to this consultation, please make this clear with your response.

If you do not give consent, the Bank may still collect, record and store it in accordance with the information provided above.

You have the right to withdraw, amend or revoke your consent at any time. If you would like to do this, please contact the Bank of England using the contact details set out below.

Responses can be sent by email to: ✉ FMI-IOREP-CP@bankofengland.co.uk.

Alternatively, please address any comments or enquiries to: Post Trade Policy Team, Financial Market Infrastructure Directorate, Bank of England 20 Moorgate, London, EC2R 6DA.

1: Overview

1.1 This consultation paper (CP) sets out the Bank of England's (the Bank's) proposals to set requirements in rules and a code of practice and expectations for UK financial market infrastructures (FMIs) to report operational incidents and their material third-party arrangements.

1.2 The Bank proposes to establish a framework for timely, accurate and consistent reporting of operational incidents, and notification and reporting of material third-party arrangements. The proposals set out clear and robust requirements and expectations for regulatory reporting which aim to support the operational resilience of the UK financial sector and enhance the Bank's understanding of sector threats and vulnerabilities.

1.3 The proposals in this CP would allow the Bank to collect data which would be used to monitor and manage potential risks arising from operational incidents and FMIs' increasing reliance on third parties in an effective but proportionate manner, and advance the Bank's objective of protecting and enhancing UK financial stability.

1.4 The rules will apply to recognised UK central counterparties (CCPs), recognised UK central securities depositories (CSDs), UK recognised payments system operators (RPSOs) and UK specified service providers (SSPs). Third-country CSDs and 'systemic third-country CCPs' are not in scope, but should HM Treasury (HMT) make regulations in future that allow for the application of these rules to third-country CSDs, or set criteria of general application in respect of the definition of a 'systemic third-country CCP', the Bank may look to expand the rules to these entities. Although non-UK RPSOs and SSPs also fall outside of the scope of these proposals, the Bank may also look to extend the rules to these entities in the future. In such circumstances, and in line with the approach set out in [**The Bank of England's approach to financial market infrastructure supervision**](#) the Bank may decide to place reliance on a home regulator where the FMI's home jurisdiction's regulatory and supervisory framework deliver broadly similar outcomes to those of the UK, and where the Bank is satisfied that there are sufficient co-operation arrangements in place and engagement to rely on the home authority.

1.5 The proposals in this CP are consistent with the approach developed jointly with the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA). The Bank has developed draft rules, a code of practice and expectations for FMIs and is seeking to implement a joint approach to the policy with the PRA and FCA. The proposals in this CP would result in:

- new rules for CCPs (Notifications and Regulatory Reporting) and CSDs (Notifications and Regulatory Reporting) and a new Part 4 (Notifications and Regulatory Reporting) of the Code of Practice for RPSOs and SSPs, as detailed in the relevant CP sections;
- a new Bank supervisory statement setting out the Bank's expectations of how FMIs should

comply with and interpret the proposed new operational incident reporting requirements in the rules and code of practice; and

- amendments to the Bank's supervisory statements on outsourcing and third-party risk management for FMIs setting out the Bank's expectations of how FMIs should comply with and interpret the proposed new material third-party arrangements requirements in the new Part 4 of the Code of Practice for RPSOs and SSPs and new rules for CCPs and CSDs.

1.6 The Bank considers that the proposals in this CP would advance its primary objective to protect and enhance the stability of the UK financial system (the Financial Stability Objective) through setting clear and robust requirements and expectations for regulatory reporting. The Bank further considers that the proposals in this CP are consistent with its new secondary objective to, where possible, facilitate innovation in the provision of CCP and CSD services when advancing the primary financial stability objective. This includes the key consideration that the reporting templates are no more prescriptive than is necessary to achieve their goals and there may be efficiency gains for FMIs in their use, freeing up resources to be used for other activities.

1.7 The Bank has a statutory duty to consult when introducing new rules and changing existing rules for CCPs and CSDs made under the Financial Services and Markets Act (FSMA) 2000.^[1] While there is not the same statutory duty to consult when introducing new codes of practice under the Banking Act 2009 or amending existing codes of practice, the Bank decided to do so in this instance to gather feedback on the proposals.

1.8 The Bank consulted the Cost Benefit Analysis (CBA) Panel on its CBA for the new rules for CCPs and CSDs on 7 November 2004. The feedback from this Panel is detailed in Appendix 7.

1.9 In carrying out its policymaking functions, the Bank is required to comply with several legal obligations. The analysis in this CP explains how the proposals have had regard to those relevant factors, including an explanation of the ways in which having regard to these factors has affected the proposals.

Background

1.10 A key priority for the Bank is to improve the operational resilience of FMIs and protect the wider financial sector from the impact of operational disruptions. As the financial sector becomes increasingly interconnected, complex and dynamic, strengthening operational resilience enables FMIs and the financial sector to more effectively deal with risks to prevent, adapt, respond to, recover, and learn from operational disruptions.

1.11 Over recent years, the Bank has undertaken a series of policy development initiatives to put in place a stronger regulatory framework to promote operational resilience. The proposals set out in this CP form part of that programme. The proposed policy would allow the Bank to collect good-quality, consistent data focusing on operational incidents and material third-party

arrangements which pose the most risk to FMIs and the financial sector. The proposals set out in this CP aim to enhance operational resilience by helping the Bank gain better oversight of these risks and provide more meaningful feedback to FMIs and the financial sector, to help address vulnerabilities and prepare for emerging risks.

1.12 In 2019, the Treasury Select Committee published a [report examining the 2018 IT failures in the financial services sector](#)^[1]. This report made a number of recommendations for UK regulators, including that the supervisory authorities should assess the accuracy and consistency of operational incident reporting data, clarify standards, guidance and definitions for industry and consider the need to expand current reporting requirements.

1.13 Following the publication of the [Bank of England policy on Operational Resilience of FMIs](#) in March 2021, increasing the operational resilience of individual FMIs and the financial system remains a priority for the Bank. To support and strengthen operational resilience, the Bank publicly committed to consider the regulatory reporting requirements for operational resilience and consult on proposals for an online portal that FMIs would populate with information about their outsourcing and third-party (OATP) arrangements.^[2]

1.14 In November 2024, the Bank, alongside the PRA and FCA, finalised its new regulatory regime for the supervision of Critical Third Parties (CTPs) to the financial sector in [PS16/24 – Operational resilience: Critical third parties to the UK financial sector](#). This regime recognises the risk that severe disruption arising from certain third parties could pose to the financial stability of the UK. To support the identification of potential CTPs and assess where critical nodes of failure could arise, the Bank needs to collect adequate data on FMIs' material third-party arrangements.^[3]

1.15 The proposals aim to ensure that FMIs submit consistent and good-quality reporting of operational incidents and material third-party arrangements by:

- **Prioritising the most significant risks to operational resilience:** by setting out clear requirements which enable FMIs to prioritise the reporting of operational incidents and material third-party arrangements which could pose risks to the delivery of an important business service (IBS), or to the financial stability of the UK.
- **Setting out standardised reporting requirements:** to enhance the quality and comparability of information submitted to the Bank on operational incidents and material third-party arrangements. This would allow the Bank to understand potential risks and vulnerabilities within the financial sector more efficiently and better identify FMIs' reliance on material third parties.

1.16 There has been increasing focus internationally on strengthening operational resilience. The policy has been designed to be as interoperable as reasonably practicable with similar existing and future regimes, such as the Financial Stability Board's (FSB's) [Format for Incident](#)

[Reporting Exchange](#) (FIRE) and the EU's [Digital Operational Resilience Act](#) (DORA).

Structure of the CP

1.17 The CP is structured into the following sections:

- Section 2 sets out proposals relating to operational incident reporting.
- Section 3 sets out proposals relating to outsourcing and third-party reporting.
- Section 4 sets out 'Have Regards' analysis for certain policy considerations.

Cost benefit analysis

1.18 The Bank is required to publish a CBA when proposing new rules for CCPs and CSDs. This is defined in s.138J FSMA 2000 as an analysis of the costs, together with an analysis of the benefits that would arise if the proposed rules are made, as well as an estimate of those costs and benefits, where reasonably practicable to do so.

1.19 The CBA was considered by the CBA Panel, which provides advice to the Bank and PRA on the preparation of cost benefit analyses, on 7 November 2024. The Panel provided feedback on the analysis of the proposals' counterfactual; the average ongoing costs of some proposals; and the analysis of the proposal's positive benefits. A summary of the Panel's comments and how the Bank responded can be found in paragraph 5 of Appendix 7.

1.20 Although the CBA requirement does not apply to the Bank's power when introducing new codes of practice under the Banking Act 2009 or amending codes of practice for RPSOs and SSPs, the Bank has carried out a proportionate CBA in respect of the proposed Code of Practice for payment systems.

Summary of benefits and costs

1.21 The CBA assesses the one-off and ongoing (annual) costs and benefits arising from the proposed framework. Based on the analysis of the costs and benefits of the proposals that are set out below, the Bank expects that the proposals would bring net benefits to the UK financial sector. The full cost benefit analysis is set out in Appendix 7.

1.22 The potential compliance costs to FMIs directly arising from the proposals reflect the incremental changes that FMIs would otherwise not have undertaken in the absence of the proposed regulation. The Bank expects there will be one-off costs to FMIs, including costs to familiarise themselves with the proposals. There would also be annual ongoing costs to FMIs to comply with the reporting requirements. In summary, the Bank estimates one-off and ongoing (annual) compliance costs of £106,500 and £41,000 respectively across all CCPs and CSDs in scope of the proposals, and similarly, one-off and ongoing (annual) compliance costs of £164,000 and £38,500 respectively across all RPSOs and SSPs in scope of the proposals.

1.23 The benefits from the proposals are expected to arise through enhanced visibility of individual FMIs' and broader financial sector operational resilience and systemic concentration risk arising from FMIs' use of third parties. Where appropriate, the Bank can use the data to work with FMIs to prioritise the mitigation of potential key vulnerabilities; and identify third parties that could be designated as critical to the financial sector. The introduction of standardised reporting guidance and reporting thresholds in relation to operational incidents and material third-party arrangements could also minimise the reporting burden and provide ongoing efficiency gains for FMIs.

1.24 The indirect benefits of the proposals include the maintenance of trust in the Bank's regulatory framework, supporting FMIs' ability to innovate within this framework, and the potential realisation of benefits from bringing Critical Third Parties into scope of the Bank's new supervisory oversight regime.

Implementation

1.25 The proposed implementation date for the proposals in this CP is no earlier than the second half of 2026.

1.26 The Bank intends for FMIs to submit operational incident reports to the Bank using the FCA's [Connect](#) portal. Connect is an online system hosted by the FCA which would enable FMIs to log in to complete the reports. The Bank notes this intention is based on its current analysis of technical reporting solutions and will continue to develop this approach ahead of the implementation date to ensure this is the most appropriate reporting platform.

1.27 The Bank intends that FMIs submit an initial version of the register of material third-party arrangements (the Register) using the FCA's [RegData](#) platform and ensure that this is up to date at least on an annual basis. The Bank notes this intention is based on its current analysis of technical reporting solutions and will continue to develop this approach ahead of the implementation date to ensure this is the most appropriate reporting platform. The Bank proposes that FMIs would submit Notifications on material third-party arrangements via electronic means.

Responses and next steps

1.28 This consultation closes on 13 March 2025. The Bank invites feedback on the proposals set out in this consultation. Please address any comments or enquiries to [✉ FMI-IOREP-CP@bankofengland.co.uk](mailto:FMI-IOREP-CP@bankofengland.co.uk).

1.29 When providing your response, please tell us whether or not you consent to the Bank publishing your name, and/or the name of your organisation, as a respondent to this CP.

1.30 Please also indicate in your response if you believe any of the proposals in this consultation paper are likely to impact persons who share protected characteristics under the Equality Act 2010, and if so, please explain which groups and what the impact on such groups might be.

2: Operational incident reporting

2.1 The proposals require FMIs to submit a report to the Bank following certain operational incidents. The Bank's proposed expectations and requirements are found in the Appendices (1, 2 and 3).

2.2 The rules and code of practice would set out specific operational incident reporting requirements for FMIs. This would include a definition of an operational incident and clear, proportionate thresholds for reporting. Under current requirements, the Bank receives inconsistent reporting from FMIs on the types and severity of incidents that occur. Similarly, the data the Bank currently receives on incidents lacks consistency, with FMIs submitting differing information, both in terms of quantity and quality, and using variable terminology to describe incidents. The purpose of these proposals is for the Bank to receive consistent, sufficient, and timely information about operational incidents which pose a risk to the Bank's objectives. This would allow the Bank to:

- assess the potential impact of operational incidents on FMIs, or on the stability of, and confidence in, the UK financial sector;
- obtain a better understanding of the operational resilience of FMIs and the financial sector; and
- identify potential vulnerabilities and areas for improvement.

2.3 The proposals in this CP set out regulatory reporting requirements for operational incidents which meet prescribed thresholds. The proposals would not replace an FMI's obligations to notify the Bank of certain incidents in accordance with:

- for CCPs: Rule 4 of the Recognised Clearing House Instrument 2018;
- for CSDs: Article 45(6) of the UK Central Securities Depositories Regulation (UK CSDR); and
- for RPSOs and SSPs: any notices issued under section 204 of the Banking Act 2009.^[4]

2.4 The Bank is also currently consulting on introducing Fundamental Rules for FMIs, including a proposed Fundamental Rule 7.^[5] This rule which would require FMIs to disclose to the Bank appropriately anything relating to the FMI of which the Bank would reasonably expect notice.

Operational incident

2.5 The operational incident reporting proposals would apply to the reporting of an 'operational incident', which is defined as either a single event or a series of linked events which disrupts an FMI's operations such that it:

- disrupts the delivery of a service to an end user external to the FMI; or
- impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to such an end user.

2.6 The Bank proposes to take a proportionate approach to operational incident reporting requirements. The proposed operational incident reporting rules would only apply in respect of operational incidents which meet one or both of the criteria referred to above as a result of a relevant disruption or impact. The reporting rule is not proposed to apply to a potential or uncrystallised event. This would have the benefit of reducing the reporting on FMIs by not requiring FMIs to report operational incidents that do not cause such a disruption or impact ('near-misses').

Reporting thresholds

2.7 The Bank proposes that FMIs would be required to report an operational incident when it meets one or more of the thresholds set by the Bank (see draft Notifications and Regulatory Reporting Parts of the proposed rules for CCPs and CSDs and the draft Notifications and Regulatory Reporting part of the proposed Code of Practice for RPSOs and SSPs (Appendix 1 and 2; and Section 3 of the draft supervisory statement in Appendix 3).

2.8 The Bank considers that thresholds must be set to ensure that it only receives operational incident data relating to operational incidents that could impact its objectives. The Bank proposes to take a proportionate approach to the reporting requirements which does not pose an undue burden on FMIs. The Bank has therefore made a decision to link the reporting thresholds to the point where an operational incident could pose a risk to its objectives.

2.9 The Bank proposes that FMIs would be required to submit an operational incident report only once an operational incident could disrupt the delivery of an FMI's IBS or otherwise pose a risk to UK financial stability.

2.10 The proposed threshold is consistent with the Bank's objectives, and the central role that FMIs play within the financial system. The Bank's current consultation on Fundamental Rules includes a proposed Fundamental Rule 10 which would require FMIs to 'identify, assess, and manage the risks that its operations could pose to the stability of the financial system'. The term 'IBS' is derived from the Bank's policy on Operational Resilience of FMIs, and should be well understood by FMIs as relating to those business services whose prolonged disruption would impact UK financial stability.

2.11 Determining which operational incidents meet the reporting threshold will be a matter of judgement for FMIs. The Bank does not propose to introduce a definitive list of operational incidents which meet the proposed threshold, as the same incidents can have varying impacts on FMIs for a range of reasons, such as differing size, business models and customer base. FMIs

may use their existing internal processes to determine the scale and potential impact of an incident and assess whether it meets the threshold for reporting. The Bank would expect FMIs to consider a range of factors when determining whether an operational incident breaches the above threshold. This could include, but is not limited to, the risk of operational or financial contagion, the FMI's ability to deliver its IBSs, and damage to the FMI's or the sector's reputation. Further details on the risks FMIs should consider are set out in the draft new supervisory statement.

2.12 A non-exhaustive list of examples of operational incidents which would meet the proposed operational incident reporting threshold has been set out in the draft new supervisory statement. These include cyber attacks, process failures, system update failures and infrastructure problems.

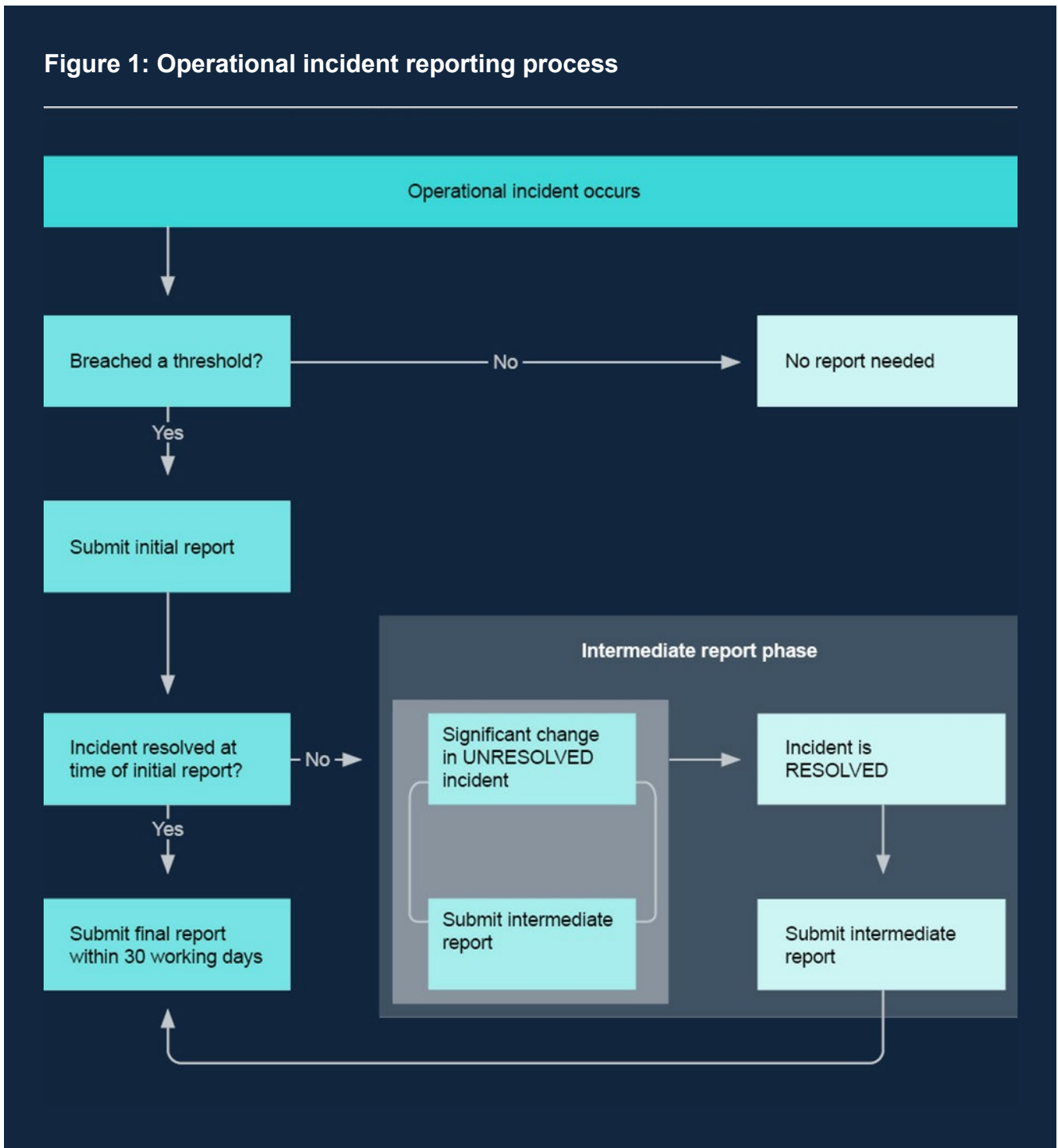
Phased approach to reporting operational incidents

2.13 When an operational incident meets the prescribed threshold, the Bank proposes to require FMIs to provide the following incident reports:

- an initial operational incident report;
- one or more intermediate operational incident reports if there is a significant change; and
- a final operational incident report.

2.14 To provide clarity on the phased approach to operational incident reporting, the process has been set out in Figure 1 below, the following sections contain further detail on the proposals for each reporting phase.

Figure 1: Operational incident reporting process



2.15 As illustrated in Figure 1, when an operational incident occurs, an FMI would be required to assess whether it has met the threshold set by the Bank. If the threshold has been met, an FMI would be required to submit an initial operational incident report as soon as is practicable after the operational incident occurs.

2.16 If the FMI has resolved the operational incident at the time of the initial report, the FMI would not need to complete the intermediate report and would instead have within 30 working days after the operational incident has been resolved to submit a final report, or where this is impracticable, as soon as is practicable but not exceeding 60 working days.

2.17 If the operational incident remains ongoing when the initial report has been submitted, the FMI would be required to submit an intermediate report(s) as soon as is practicable after there is a significant change in the circumstances of the incident as reported in the previous incident report made to the Bank.

2.18 As soon as practicable after the incident has been resolved, the FMI would be required to submit an intermediate report informing the supervisory authorities of this change and would then have within 30 working days after the operational incident has been resolved to submit the final report, or where this is impracticable, as soon as is practicable but not exceeding 60 working days.

2.19 The Bank's proposed phased and incremental approach to operational incident reporting is aligned to international standards proposed through the FSB's FIRE.

Initial operational incident report

2.20 The Bank recognises the need to balance the objectives of receiving timely operational incident information to understand potential risks to its statutory objectives and FMIs taking actions to resolve the incident. Therefore, rather than setting a minimum time, the Bank proposes to require FMIs to submit an initial incident report as soon as practicable after the operational incident has met the proposed reporting threshold. The Bank would expect that an FMI submit the report within 24 hours.

2.21 To limit the burden posed to an FMI at a time when it should be focused on managing the operational incident, FMIs would only be required to submit a limited set of information within this initial incident report to allow the Bank to gain an understanding of the incident and assess potential risks to its objectives.

Intermediate operational incident report

2.22 FMIs would be required to submit an intermediate operational incident report as soon as is practicable after there is a significant change in the circumstances described in the most recent report submitted to the Bank. This could include, but is not limited to, a change in the impact of the operational incident or the status of the operational incident, such as the FMI identifying the origin of the operational incident; and the FMI resolving the operational incident. A non-exhaustive list of examples of when the intermediate report should be submitted is set out in the draft new supervisory statement.

2.23 An FMI would be required to submit multiple intermediate reports if numerous significant changes occur. At a minimum, where an operational incident is not resolved at the time of the initial report, an FMI would be required to complete one intermediate report to inform the Bank that it has resolved the operational incident.

2.24 In the event that an FMI has resolved an incident prior to submitting an initial report, they would not be required to complete an intermediate report and can move straight to the final report stage. The FMI would be required to let the Bank know that the incident has been resolved as soon as practicable within the initial report (which the FMI must submit as soon as practicable as set out above) and follow up with the final incident report as required.

Final operational incident report

2.25 An FMI would be required to submit a final operational incident report within 30 working days after the operational incident has been resolved or, where this is not practicable, as soon as is practicable but not exceeding 60 days. Where it is impracticable to submit the final report within 30 working days, FMIs would be expected to contact the Bank explaining the reason as to why it is impracticable and the expected timeframe for the submission of the final report. The Bank proposes that the final report include a full assessment of the impact of the incident, the lessons learned and the identified root causes.

Format of operational incident reports

2.26 The Bank intends that FMIs submit incidents reports through the FCA's [Connect](#) portal. Connect is an online system hosted by the FCA which would enable FMIs to log in to complete the prescribed reports.

2.27 FMIs would be required to complete the information set out in the reporting fields document found in Appendix 8 for each type of operational incident report. To minimise FMIs' reporting burden where relevant, the Bank has considered the FSB's FIRE and the EU's DORA, and aligned the reports where possible.

Operational incident data

2.28 The Bank proposes that FMIs submit reports on operational incidents in a template which would include four data categories (see Table A). The level of information required would vary depending on the stage of the reporting, with progressively more expected as the incident progresses or is closed.

2.29 As noted above, the proposed template has been developed with regard to the proposals being consulted on under the FSB's FIRE, including alignment with the format of data fields and taxonomies which underpin these where appropriate. The Bank has also, where possible, aligned specific data fields and underpinning taxonomies between the operational incident reporting and material third-party reporting templates (see Section 3) to enable data set interaction. This could support the Bank's identification of incident contagion where an incident originates at a third party, and enable it to, where appropriate, alert other FMIs of these risks.

Table A: Data categories for operational incident reporting

Data category	Description
Reporting details	Details of the firm reporting the incident, including contact information, firm identification, and the receiving authority.
Incident details	Details of the operational incident including incident status, incident description, service disrupted, time of incident and actions the firm intends to take/has taken to recover.
Impact assessment	Information regarding the impact of the operational incident, including number of customers/clients affected, reputational impact, volume and value of transactions affected, and parties affected.
Incident closure	Information on the root cause(s), lessons learned and subsequent remedial actions.


2.30 Reporting details: To ensure the Bank has up-to-date and correct information on the FMI reporting the operational incident, FMIs would be required to complete a section on reporting details. This would include data relating to the reporting entity's details, contact information, incident identification and the receiving authority details. FMIs would only be required to complete these details in the initial report phase, and subsequent reports would be pre-populated with this information.

2.31 Incident details: FMIs would be required to complete the operational incident details section so the Bank understands the nature of the incident, any service impacted and what actions the FMI may be taking, or has taken, to resolve the incident. FMIs would be required to submit these data items at the initial report phase and can amend these in the intermediate and final report phases.

2.32 Impact assessment: To ensure the Bank understands the full impact of an operational incident on the FMI, its participants and their clients (if relevant) and the broader financial sector, FMIs would be required to complete the impact assessment section. The required fields for this category vary depending on the stage of the reporting. For example, the initial incident report requires limited information on the initial assessment and initial remedial actions. The final incident report includes additional fields to provide a more comprehensive reporting of the incident, including service disruption type and duration and resources affected. Most impact assessment fields would however be available for FMIs to optionally complete if they have the information to do so.

2.33 Incident closure: The Bank would require FMIs to submit information on incident closure in

the final report phase. This would allow the Bank to understand the actions the FMI has taken or needs to take to address and remediate possible risks and vulnerabilities to the FMI and the financial sector.

2.34 The proposed list underpinning the business services data fields is based on the critical economic functions set out in [SS 19/13 – Resolution planning](#) and the critical functions set out in the [FSB Guidance on Identification of Critical Functions and Critical Shared Services](#) . We believe that this list is appropriate for FMIs, and it is aligned with the proposals for the material third-party reporting templates below in Section 3. The proposed list underpinning the root cause data fields is based on the FCA Root Cause component list, which has historically been used by the FCA to manage and triage notified incidents.

2.35 The Bank proposes to include some data fields which would be required conditionally depending on the type of operational incident. For example, where an operational incident originates at a third party, an FMI would be required to provide further information relating to the third party. In such situations, the Bank proposes that an FMI take reasonable steps to obtain information regarding the root cause of the incident from the third party.

Statutory obligations

2.36 In carrying out policymaking functions the Bank is required to comply with several statutory obligations. This section explains how the Bank has had regard to the obligations applicable to the Bank's policy development process, including an explanation of how this is reflected in Section 2 of this CP relating to the operational incident reporting proposals.

Statutory objectives analysis

2.37 The Bank has developed the proposals for operational incident reporting rules for CCPs and CSDs in accordance with the relevant statutory obligations in the Bank of England Act 1998 and FSMA 2000 (as amended by FSMA 2023). This includes considering the proposals against the Bank's Financial Stability Objective and its secondary objective to facilitate innovation in the provision of FMI services^[6] (the Secondary Innovation Objective), as well as the requirement to 'have regard' to certain policy considerations and to carry out a CBA.

2.38 The Bank has developed the proposals for an operational incident reporting Code of Practice for RPSOs and SSPs under the legislative framework set out in Part 5 of the Banking Act 2009. While these require considering the proposals against the Financial Stability Objective, it does not include a requirement to consider them against the secondary innovation objective, to expressly 'have regard' to certain policy considerations or to carry out a CBA in the same manner as the accountability framework for CCPs and CSDs. However, the Bank has included RPSOs and SSPs in the CBA for the proposals on a non-statutory basis.

2.39 This section outlines the analysis of the operational incident reporting rules against these

frameworks, making clear where it applies to all FMIs, or only to CCPs and CSDs, or only RPSOs and SSPs.

Financial stability objective – all FMIs

2.40 The Bank's proposals are designed to advance its primary objective to protect and enhance the stability of the financial system. By collecting timely, structured and accurate information on operational incidents, the Bank can better monitor and assess individual FMIs' and the broader sector's operational resilience. Consistent data can enable the Bank to provide meaningful feedback to industry to help address vulnerabilities and prepare for emerging risks within the sector.

Secondary innovation objective – CCPs and CSDs

2.41 The Bank considers that the operational incident reporting proposals are compatible with the Bank's secondary objective for CCP and CSD rulemaking to facilitate innovation in the provision of FMI services so far as reasonably possible.

2.42 The Bank intends to reduce compliance burden and ensure FMIs can efficiently allocate resources for reporting through the introduction of clear reporting thresholds, standardised reporting templates, and developing a single reporting solution to work across authorities. Although the approach is prescriptive, this is necessary to achieve the desired outcome. Through introducing a streamlined and standardised reporting process it should support FMIs in allocating resources to other innovative activities.

2.43 The Bank considers that by collecting good-quality data on operational vulnerabilities, the Bank would be in an improved position where it can work more effectively with FMIs to manage vulnerabilities and prepare for emerging risks. This can increase confidence within the market and facilitate the Bank maintaining trust in its regulatory framework, which supports FMIs' ability to innovate within that framework.

Equality and diversity – all FMIs

2.44 In developing its proposals, the Bank has had due regard to the equality objectives under s.149 of the Equality Act 2010. The Bank considers that the proposals do not give rise to equality and diversity implications.

3: Outsourcing and third-party reporting

3.1 In this section, the Bank is proposing to:

- expand the scope of existing third-party arrangements data collection to cover both material outsourcing and non-outsourcing ('material third-party') arrangements;
- require FMIs to submit material third-party Notifications in a standardised format, using a template which is aligned with the proposed Register; and
- require FMIs to maintain and submit a Register to the Bank, ensuring this is updated at least annually.

3.2 The proposals in this section would result in:

- New rules for CCPs (Notifications and Regulatory Reporting) and CSDs (Notifications and Regulatory Reporting), and a new Part 4 (Notifications and Regulatory Reporting) of the Code of Practice for RPSOs and SSPs, as detailed in the relevant CP sections.
- Amendments to the Bank's supervisory statements on outsourcing and third-party risk management for FMIs.

3.3 FMIs are becoming increasingly reliant on third-party arrangements, both outsourcing and non-outsourcing, to support their operations and the delivery of their FMI services. The reliance on third-party arrangements brings potential benefits and opportunities for the sector but could also pose risks to the financial stability of the UK. To better identify and address these risks, the regulators and the industry have highlighted the importance of collecting effective data on the use of material third-party arrangements.

3.4 There are currently a variety of existing requirements or expectations for FMIs to notify or seek approval from the Bank for outsourcing arrangements, and for FMIs to keep records of such arrangements. CCPs and CSDs are required by the UK European Market Infrastructure Regulation (UK EMIR) and UK CSDR to seek the Bank's approval before entering into major outsourcing arrangements. Similarly, RPSOs and SSPs are required by the outsourcing and third-party risk management part of the Bank's Code of Practice to notify the Bank before entering into any new outsourcing agreement. All FMIs are subject to the expectation in the Bank's supervisory statements on outsourcing and critical third-party risk management for FMIs. This includes that they keep appropriate records of their outsourcing and third-party arrangements, and notify the Bank and seek the Bank's non-objection when entering into or significantly changing a critical outsourcing or third-party arrangement, or when there is a material change in their risk profile and that of the services they provide.

3.5 Although these requirements provide valuable information to the Bank, they are not established on a consistent statutory basis across the FMI regimes, and the notifications process is unstructured, which can limit the value of the data. In addition, there is no formal requirement for CCPs and CSDs to maintain a register of such arrangements and submit it to the Bank, further limiting the ability of the Bank to understand current third-party arrangements across FMIs.

3.6 The proposals seek to address these gaps by providing clear and consistent requirements and expectations for the collection of data on material third-party arrangements.

Material third-party arrangements

3.7 As FMIs' operations have become more complex and dependent on technology over recent years, FMIs are becoming increasingly reliant on a wider range of services delivered by third-party providers. To support their operational resilience, FMIs need to effectively manage risks posed by their third-party arrangements. To help achieve this, the Bank proposes to introduce new requirements for all FMIs to maintain and submit to the Bank a register of all 'material third-party arrangements' that they have entered into and update it annually, as well as notify the Bank when entering into new material third-party arrangements or significantly changing existing arrangements. The proposals aim to aid the Bank in better identifying systemic risks posed by third-party service providers and support the Bank's recommendation of potential CTPs to be designated by HMT.

3.8 The Bank proposes to define a 'material third-party arrangement' as a third-party arrangement which is of such importance that a disruption or failure in the performance of the product or service provided to the FMI could pose a risk to the continuity of service provided by the FMI; or in the case of:

- a CCP, the safety and efficiency of the CCP's clearing services;
- a CSD, the safety and efficiency of the CSD's securities settlement systems;
- a RPSO, the safety and efficiency of the payment systems operated by the RPSO; or
- a SSP, the safety and efficiency of the payment systems to which the SSP provides services.

3.9 This is irrespective of whether the relationship is an outsourced or non-outsourced arrangement. This definition is consistent with the existing definition of 'critical third party' in the Bank's supervisory statements on outsourcing and third-party risk management and critical third parties for FMIs.

3.10 We further propose to amend those supervisory statements to replace the term 'critical third party' with 'material third-party arrangement' to avoid any confusion that may arise with the use of the term 'Critical Third Party' by the Bank, PRA and FCA's policies on 'Operational Resilience: Critical Third Parties to the UK Financial Sector'.^[7] We also propose to amend those same supervisory statements to replace the term 'critical outsourcing arrangement' with 'material

outsourcing arrangement', to ensure consistency in that document.

3.11 The Bank has chosen to make use of the existing interpretation of 'critical third-party arrangements' as it is well understood by FMIs, and proportionate to requiring notification to the Bank of those arrangements that are potentially most impactful to UK financial stability. It is also consistent with complementing the existing expectation on FMIs to notify the Bank and seek the Bank's non-objection in respect of 'critical third-party arrangements' (which, as above, would be replaced with the term 'material third-party arrangements') with requiring FMIs to maintain a register of such arrangements and to notify the Bank appropriately.

3.12 Although the term 'material third-party arrangements' is the same term as that proposed by the PRA in its consultation paper on 'Operational Resilience: Incident and Outsourcing and Third-Party Reporting' and captures a similar set of activities, the Bank's proposed rules contain a different definition applicable to FMIs as set out above.

Notifications

3.13 In line with the existing approach, and to ensure the Bank collects relevant information at a proportionate cost to FMIs, the Bank proposes to only collect information on FMIs' material third-party arrangements.

3.14 The Bank proposes to introduce a new requirement for FMIs to notify the Bank in a prescribed form when they enter into or significantly change material third-party arrangements (as defined above). This will standardise the way FMIs submit such notifications through the use of a standardised template, supported by additional documentation where necessary. The introduction of a template which provides clear expectations on the minimum information expected in material third-party notifications is intended to reduce FMIs' reporting burden. The Bank would use these notifications to inform its conduct of any necessary supervisory scrutiny and have adequate oversight of FMIs and review relevant material third-party arrangements in respect of any risks to its objectives.

3.15 For CCPs and CSDs this would formalise the existing expectation to notify the Bank when they enter into critical third-party arrangements, as established in the Bank's supervisory statements on outsourcing and critical third-party risk management for FMIs.

3.16 For RPSOs and SSPs, it would complement the existing requirement to notify the Bank prior to entering into any new outsourcing agreements as set out in Part 3 of its Code of Practice. For all FMI types, it would introduce a new requirement to submit these notifications in a standardised format to the Bank through electronic means.

3.17 For CCPs and CSDs this will be done by the introduction of new rules, and for RPSOs and SSPs, this will be done through a new Part 4 of the Code of Practice.

3.18 The information the Bank proposes to collect on FMIs' material third-party arrangements is specified in Table B below.

Register

3.19 As set out in the Bank's [outsourcing and third party risk management supervisory statements for FMIs](#), and to reflect the proposals outlined above, the Bank proposes to require FMIs to maintain and submit a structured register of information on their material third-party arrangements to the Bank (Register). This would formalise and expand the existing expectations and requirements that FMIs should maintain records of their outsourcing and third-party arrangements. This would result in additional rules in the Notifications and Regulatory Reporting parts for CCPs and CSDs set out in Appendix 1 and a new Part 4 of the Code of Practice (Notifications and Regulatory Reporting) set out in Appendix 2.

3.20 The Bank considers that, in complying with the existing expectations contained in the Bank's supervisory statements on outsourcing and critical third-party risk management for FMIs, FMIs would likely already have records of their material third-party arrangements for this purpose. The Bank has also been collecting a similar register of information from FMIs on a voluntary ad-hoc basis since 2023.

3.21 The Bank intends to require FMIs to submit the Register using the FCA RegData platform once and then ensure that this is up to date at least on an annual basis. To update the Register, FMIs may re-upload the complete Register itself or amend the Register using the functionality provided by the RegData platform.

3.22 The Bank considers that collecting data on FMIs' third-party arrangements in a consistently structured format through a central register supports the Bank's statutory functions to protect and enhance UK financial stability. The Bank proposes to use the data collected in the Register to:

- monitor and address systemic concentration risk in non-regulated third-party arrangements;
- efficiently identify third parties which could be considered appropriate for recommendation to HMT for designation as CTPs;
- assess FMIs' compliance with the existing expectations and requirements in the Bank's outsourcing and third-party risk management policy for FMIs;
- collect supervisory insights on individual FMI's level of third-party usage;
- where appropriate, share anonymised aggregated findings on industry-wide trends; and
- determine contagion risk of operational incidents when FMIs report incidents caused by third-party disruption.

3.23 The information that the Bank proposes to collect on FMIs' material third-party arrangements is specified in Table B below.

Information to submit to the Bank

3.24 To minimise FMIs' reporting burden, the Bank has developed the proposed templates for the Notifications and Register to be aligned with each other. The Bank has developed the templates predominantly using existing Register templates that have been used for previous Bank outsourcing data collections as a basis. To provide consistency and reduce reporting burden on FMIs, the Bank has developed its proposed templates to be interoperable where practicable with similar existing and future regimes, such as the EU's DORA.

3.25 The data that the Bank proposes to collect is summarised in Table B below. The full proposed template and guidance are set out in Appendix 9. The proposed template features standardised data items which are underpinned by certain taxonomies to increase reporting efficiencies and limit free text fields. The Bank has also aligned specific data fields and underpinning taxonomies between the operational incident reporting and material third-party reporting templates to enable data set interaction. This could support the Bank's identification of incident contagion where an incident originates at a third party, and enable it to, where appropriate, alert other FMIs of these risks.

Table B: Proposed data field categories to be collected

Data group	Description
Master data on firm submission	Information on submission references, such as type and date of submission.
Master data on regulated firms	Details on the firm submitting material third-party arrangement information, including firm identification.
Master data on external product or service provider, including intragroup arrangements	Details of the external product or service provider firms have an arrangement with, including the name, registered address, and legal identifiers of the product or service provider.
Data on types of products or services being performed by an external provider	Information on the products or services being provided by an external provider, including the type and a description of the product or service, whether the product or service supports an IBS, and the country where the product or service is being performed.
Information on supply chain	Ranking of external providers for each product or service included in the scope of each contractual arrangement.
Data on assessments	Information on firms' due diligence conducted for each arrangement, including details on risk assessments, recent audits, and governance reviews.

3.26 The proposed template is comprised of six data groups, which are underpinned by specific taxonomies and are linked to each other using specific keys to form a relational structure, that enables the Bank to form a view of third-party supply chains. These include the firm identifier, contractual arrangement reference numbers, third-party provider name and legal entity identifiers, and the supply chain rankings.

3.27 FMIs would be required to submit high-level data relating to their reporting entity details and third-party arrangements, to enable the Bank to distinguish each Register or Notification submission. This data would include submission identifiers, firm reference numbers, and contractual arrangement numbers.

3.28 To enable the Bank to assess the extent of the concentration of third-party providers supporting specific FMI business services or products, FMIs would be required to submit data relating to the types of services being performed by a third party, including whether this is an IBS for the FMI. The proposed list underpinning the business services data field is based on the critical economic functions set out in [SS 19/13 – Resolution planning](#) and the critical functions set out in the [FSB Guidance on Identification of Critical Functions and Critical Shared Services](#) [↗](#). As noted above, we believe that this list is appropriate for FMIs, and it is aligned with the proposals for the operational incident reporting templates in Section 2.

3.29 To allow the Bank to conduct structured analysis on the types of externally provided products and services FMIs use, FMIs would be required to indicate these from a pre-defined list. The proposed list underpinning this data field is based on the [DORA Final Report on draft Implementing Technical Standards \(ITS\) on Register of Information – Annex III Type of Information and Communication Technology \(ICT\) service taxonomy](#) [↗](#), which has been modified to include additional relevant non-ICT services.

3.30 To support the Bank's understanding of an FMI's third-party supply chain, FMIs would be required to 'rank' the position of each product or service provider within its supply chain. This is used to link each external provider included in the scope of each contractual arrangement supply chain. The first external service provider that an FMI is purchasing from directly would always have a 'rank' number of '1', with lower numbers denoting the closeness of the arrangement to the FMI (eg providers with rank '2' would be an external provider's supplier).

3.31 For consolidated group submissions, FMIs would be required to link each external provider to the individual regulated entity receiving the product or service. Intragroup arrangements do not generally constitute as being externally provided, so the 'rank' to be reported should be '0'.

3.32 To ensure a proportionate approach, the Bank proposes to only require FMIs to identify service providers within the supply chain whose disruption would impair the continuity of the FMI's service irrespective of the rank. This is broadly aligned with the approach taken in the EU's

DORA. This would allow the Bank to link all material third-party product or service providers who are part of the same supply chain and can indicate where 'nth' party^[8] concentration risks may arise.

3.33 The Bank also proposes to require FMIs to submit some basic information relating to their assessments of material third-party arrangements to assess FMIs' compliance with the expectations set out in the Bank's supervisory statements on outsourcing and third-party risk management.

Statutory obligations

3.34 In carrying out policymaking functions the Bank is required to comply with several statutory accountability obligations. This section explains how the Bank has had regard to the obligations applicable to the Bank's policy development process, including an explanation of how this is reflected in the proposals in Section 3 of this CP relating to material third-party arrangements.

Statutory objectives analysis

3.35 The Bank has developed the proposals for material third-party reporting rules for CCPs and CSDs in accordance with the relevant statutory obligations in the Bank of England Act 1998 and FSMA 2000 (as amended by FSMA 2023). This includes considering the proposals against the Bank's Financial Stability Objective and its secondary objective to facilitate innovation in the provision of FMI services (the Secondary Innovation Objective), as well as the requirement to 'have regard' to certain policy considerations and to carry out a CBA.

3.36 The Bank has developed the proposals to amend the outsourcing and third-party reporting part of the Code of Practice for RPSOs and SSPs under the legislative framework set out in Part 5 of the Banking Act 2009. While these require considering the proposals against the Financial Stability Objective, it does not include a requirement to consider them against the secondary innovation objective, to expressly 'have regard' to certain policy considerations or to carry out a CBA in the same manner as the accountability framework for CCPs and CSDs. However, the Bank has included RPSOs and SSPs in the CBA for the proposals on a non-statutory basis.

3.37 This section outlines the analysis of the material third-party arrangement proposals against these frameworks, making clear where it applies to all FMIs, or only to CCPs and CSDs, or only RPSOs and SSPs.

Financial stability objective – all FMIs

3.38 The Bank's proposals are designed to advance its primary objective to protect and enhance UK financial stability. Collecting consistent and structured data on FMIs' material third-party arrangements would enable the Bank to identify and support the oversight of potential CTPs in the financial sector. The Bank can also better monitor emerging risks and determine incident

contagion risks where these originate from third-party providers. The data collected can also support the Bank's supervision of FMIs' performance against the expectations set out in the relevant supervisory statements and the outsourcing and third-party risk management part of the Code of Practice, and support FMIs to address potential gaps to improve their risk management.

Secondary innovation objective – CCPs and CSDs

3.39 The Bank considers that the material third-party reporting proposals are compatible with the Bank's secondary objective to facilitate innovation in the provision of FMI services so far as reasonably possible.

3.40 The Bank intends to reduce compliance burden and ensure FMIs can efficiently allocate resources for reporting through the introduction of clear reporting thresholds, standardised reporting templates, and developing a single reporting solution to work across authorities. Although the approach is prescriptive, this is necessary to achieve the desired outcome. Through introducing a streamlined and standardised reporting process it should support FMIs in allocating resources to other innovative activities.

3.41 The Bank considers that by collecting good-quality data on material third-party arrangements, the Bank would be in an improved position where it can work more effectively with FMIs to manage third-party risks. The data would also support the Bank's oversight of potential CTPs in the financial sector, which in turn can help to increase the long-term system-wide resilience of the financial sector. This can increase confidence within the market and promote broader UK financial stability, which supports FMIs' ability to innovate within that framework.

Equality and diversity – all FMIs

3.42 In developing its proposals, the Bank has had due regard to the equality objectives under s.149 of the Equality Act 2010. The Bank considers that the proposals do not give rise to equality and diversity implications.

4: Have regards analysis

4.1 When making policy for CCPs and CSDs, the Bank must 'have regard' to certain public policy considerations set out in the Bank of England Act 1998 as amended by FSMA 2023.^[9] The Bank has had regard to these considerations, and the following 'have regards' are the ones it considers significant to the proposed rules. Where analysis has not been provided against a 'have regard', it is because the Bank considers that 'have regard' to not be a significant factor for the proposals in this CP.

1. The principle that the Bank should exercise its FMI functions as transparently as possible.

4.2 The rule-based requirements increase transparency and clarity to FMIs of the Bank's reporting requirements which should decrease resourcing and costs over time.

2. The need to use the resources of the Bank efficiently.

4.3 The Bank is proposing the introduction of standardised reporting requirements and a single reporting solution for incident and material third-party arrangement reporting which would work across authorities. Collecting structured data through a simplified reporting solution would enable the Bank to use its resources to efficiently process this, conduct incident analysis and support the supervision of operational resilience and the implementation of the CTP oversight regime.

3. The principle that a burden or restriction which is imposed on a person, or on the carrying on of an activity, should be proportionate to the benefits, considered in general terms, which are expected to result from the imposition of that burden or restriction.

- The Bank considers that the proposed reporting burden on FMIs is reduced through the use of clear reporting requirements and the introduction of standardised templates.
- The Bank considers the proposals are convergent with the standards set out as proposed by the FSB's FIRE, particularly to reduce regulatory reporting burden for FMIs with reporting obligations in multiple jurisdictions.
- In collecting consistent and structured incident reporting data, the Bank can better monitor individual FMIs' and wider financial sector operational resilience and prepare for potential emerging risks, which it can subsequently share back with industry to address vulnerabilities.

4. The desirability where appropriate of the Bank exercising its FMI functions in a way that recognises differences in the nature of, and objectives of, businesses carried on by different persons.


- The proposed reporting thresholds would limit the reports FMI submit to the Bank on incidents that pose a risk to UK financial stability, including the delivery of FMI's IBS. Taking this approach also enables FMI to make judgements based on their individual business models.

5. The effects generally that the exercise of FMI functions will or may have on the financial stability of countries or territories (other than the United Kingdom) in which FMI entities are established or provide services.

- The proposals improve oversight of FMI and sector-wide operational resilience and allow the Bank to proactively identify emerging systemic risks and take appropriate action, which will support the financial stability of the countries in which the FMI's participants are established.

Appendices

Appendix 1: Draft notification of third-party arrangements and operational incident reporting rules for CCPs and CSDs

[Draft notification of third-party arrangements and operational incident reporting rules for CCPs and CSDs](#) 

Appendix 2: Draft amendments to the payment systems code of practice: notification of third-party arrangements and operational incident for RPSOs and SSPs

[Draft amendments to the payment systems code of practice: notification of third-party arrangements and operational incident for RPSOs and SSPs](#) 

Appendix 3: Draft operational incident reporting supervisory statement

1: Introduction

1.1 This supervisory statement (SS) sets out the Bank's expectations of how UK financial market infrastructures (FMIs) should comply with the Bank's requirements for reporting an operational incident.

1.2 These requirements seek to support the operational resilience of the UK financial sector by collecting information from FMIs on operational incidents which could disrupt the FMIs' provision of its important business services (IBS) or pose a risk to UK financial stability. Further, the aim of the operational incident reporting policy is to set out clear and consistent reporting requirements and expectations for FMIs for when they experience an operational incident.

1.3 The rules underpinning these supervisory expectations apply to recognised UK central counterparties (CCPs), recognised UK central securities depositories (CSDs), UK recognised payments system operators (RPSOs) and UK specified service providers (SSPs).

1.4 The expectations set out in this SS should be read in conjunction with:

- Notifications and Regulatory Reporting rules for CCPs/CSDs.
- The Notifications and Regulatory Reporting part of the Code of Practice (CoP) for RPSOs/SSPs.
- The Bank's supervisory statements on 'Operational resilience: impact tolerances for important

business services’.

Structure of this supervisory statement

- Section 2 – establishes the definitions used in the SS.
- Section 3 – sets out how an FMI should comply with the operational incident reporting threshold requirements.
- Section 4 – sets out how an FMI should comply with the phased approach to operational incident reporting.

2: Definitions

Important business services

2.1 ‘Important business services’ is defined in the glossary of the FMI Rulebook for CCPs and CSDs and section 1.3 in Part 3 of the Code of Practice for RPSOs and SSPs. For CCPs and CSDs, it means a service which, if disrupted for a prolonged period, would pose a risk to the stability of the UK financial system by significantly disrupting the orderly functioning of a market to which a CCP or CSD provides that service.

2.2 For RPSOs it means a service provided to an end user which, if disrupted, could threaten the transfer of payments or safety and efficiency of a payment system. For SSPs, it means, a service provided by a SSP to a RPSO which, if disrupted, could threaten the transfer of payments or safety and efficiency of the RPSO.

3: Operational incident reporting thresholds

3.1 This section sets out the Bank’s expectations for how FMIs should interpret the thresholds set out in the Notifications and Regulatory Reporting Part of the CCP and CSD rulebook, and in the Notifications and Regulatory Reporting Part of the Code of Practice for RPSOs and SSPs.

3.2 FMIs must submit an operational incident report in the event that an operational incident could disrupt the provision of an important business service for a prolonged period or otherwise pose a risk to the stability of the UK financial system.

3.3 When assessing whether an operational incident meets the threshold and must be reported to the Bank, the Bank would expect FMIs to consider a range of factors. These could include, but are not limited to:

- Operational and financial contagion.
- The FMI’s ability to deliver its important business services.
- The FMI’s or the sector’s reputation.
- The FMI’s ability to meet its legal and regulatory obligations.
- The FMI’s ability to safeguard the availability, authenticity, integrity or confidentiality of data or

information relating or belonging to an end user external to the FMI.

These elements are covered in more detail in the following sub-sections.

3.4 Examples of operational incidents which the Bank would expect FMIs to report include, but are not limited to:

Cyber attacks, such as:

- A phishing attack on an FMI which compromises the confidentiality of sensitive or critical data belonging to an end user external to the FMI.
- A large-scale distributed denial of service (DDoS) attack on a cloud service provider which causes significant disruption to the delivery of one or more of an FMI's services.

Process failures which significantly disrupt the delivery of a service, for example, in the case of a CCP, the prevention or delay in issuing settlement instructions or register trade. Alternatively, these could cover a system failure that requires a manual workaround, which could in turn lead to a greater possibility of error in the processes being delivered.

System update failures which result in significant disruption of one or more services, for example, in the case of payment systems, the FMI being unable to process a significant number of transactions. This could also capture an update that allows an important business service to continue functioning but increases its vulnerability to cyber attacks.

Infrastructure problems, including extended power outages or infrastructure damage from extreme weather, which results in an FMI being unable to provide one or more of its services. For example, a physical break in a fibre connection at a site resulting in an FMI's online services being unavailable for an extended period.

The FMI's ability to deliver its important business services

3.5 Chapter 4 of the Notifications and Regulatory Reporting Part for CCPs and CSDs and Rule 4 of the Notifications and Regulatory Reporting part of the CoP for RPSOs and SSPs requires FMIs to submit an operational incident report where an operational incident could disrupt their delivery of its important business services for a prolonged period. An FMI is expected to consider whether disruption arising from an operational incident is such that its ability to deliver its important business services adequately may be called into question, leading to potential loss of business and damaging revenues.

3.6 This could include, but is not limited to:

- The FMI being unable to provide an important business service (or services) for an extended period of time;
- The FMI being unable to meet contractual obligations;

- The FMI being unable to complete or process a significant number of transactions;
- A disruption causing mounting detriment or actual harm to participants or counterparties.

3.7 FMIs should also consider whether to report those operational incidents that pose a risk to delivery of its other services, including where these could impact on its ability to deliver its important business services adequately, thereby impacting UK financial stability.

Operational and financial contagion

3.8 FMIs are required to submit an operational incident report when an operational incident could pose a risk to financial stability. As set out in [the FPC's macroprudential approach to operational resilience](#), when determining the potential impact on financial stability, FMIs are expected to consider whether there is a risk of operational contagion or financial contagion.

3.9 The Bank expects FMIs to consider operational contagion, where an operational incident could cause operational disruption elsewhere in the financial system or the real economy. An operational incident affecting the services of an FMI could leave them unable to transact with other firms or participate in financial markets. This could have knock-on impacts to the ability of the disrupted FMI's counterparties to undertake their own activities.

3.10 FMIs should consider whether an operational incident could result in further financial impacts on the FMI or the financial sector. This includes, but is not limited to, an impact on liquidity flows, access to funding sources, price discovery in certain markets or for particular assets, or a firm's ability to make margin payments to a CCP, triggering default proceedings.

The FMI's or the sector's reputation

3.11 FMIs are expected to submit an operational incident report where an operational incident risks its own reputation or the reputation of the financial sector, therefore impacting financial stability.

3.12 FMIs should consider whether an operational incident could result in a loss of confidence in the FMI itself or the wider financial sector. This could include, where an operational incident causes a FMIs' participants or financial counterparties to revise their view of the FMI, the riskiness of the FMI, its ability to manage its risks and the risks to its business model, or the strength of the financial market.

3.13 As part of its assessment of whether an operational incident should be reported to the Bank, FMIs should consider whether the incident has, or is likely to:

- have significant coverage in the media, including, but not limited to, social media, local and national news;
- lead to the FMI receiving multiple complaints from participants or financial counterparties;
- risk the FMI losing participants or financial counterparties with a material impact on its

business because of the incident.

The FMI's ability to meet its legal and regulatory obligations

3.14 The Bank expects an FMI to submit an incident report where an operational incident could result in the FMI failing to meet its legal and regulatory obligations.

3.15 In judging whether to submit an incident report, FMIs are expected to consider whether the operational incident would lead to heightened regulatory monitoring, formal regulatory action, or authority intervention.

The FMI's ability to safeguard the availability, authenticity, integrity or confidentiality of assets relating or belonging to an end user external to the FMI

3.16 The Bank expects an FMI to submit an operational incident report where an operational incident could compromise the FMI's ability to safeguard information and data belonging to an end user external to the FMI. This would include data or information:

- becoming temporarily or permanently inaccessible or unusable;
- having questionable authenticity, for example, a data source becoming untrustworthy;
- becoming inaccurate or incomplete;
- being accessed by or disclosed to an unauthorised party or system.

3.17 Examples include, but are not limited to, unauthorised access to data or a loss in sensitive data belonging to an end user external to the FMI, a cyber-attack on the FMI, or an internal service error resulting in a loss of data belonging or relating to an end user external to the FMI.

The FMI's internal assessment and classification of the incident

3.18 An FMI must submit an operational incident report where the operational incident meets the threshold set by the Bank. Where an FMI has assessed an operational incident as high priority according to its own internal procedures, this may be indicative that the Bank's threshold has been met. Additionally, where an operational incident has resulted in a high level of internal escalation, such as, to the Board, this is also likely to be indicative that the Bank's threshold has been met.

4: Approach to phased incident reporting

4.1 When an operational incident meets the prescribed threshold, as set out under Rule 4.1 of the Notifications and Regulatory Reporting Parts for CCPs and CSDs of the FMI Rulebook and the Regulatory Reporting Part of the Code of Practice for RPSOs and SSPs, an FMI is required to submit the following incident reports:

- an initial incident report,

- one or more intermediate reports if there has been a significant change to the circumstances outlined in the initial report; and
- a final report.

4.2 Under Rules 4.1–4.5 of the CCP and CSD rules and of the Code of Practice for RPSOs and SSPs, an FMI is required to complete specified information in the incident reports. FMIs are able to provide optional further information in the report where relevant. If an incident originates at a third party, the Bank expects an FMI to take reasonable steps to obtain information regarding the root cause of the incident from the third party.

4.3 An FMI must submit the relevant incident report to the Bank, as stated in Rules 4.1–4.3 of the CCP and CSD rules and of the Code of Practice for RPSOs and SSPs. FMIs are expected to use the FCA Connect portal to complete the submission.

Initial operational incident report

4.4 The Notifications and Regulatory Reporting Parts require FMIs to submit an incident report as soon as practicable after an operational incident has occurred and meets one or more of the thresholds in Rule 4.1 of the CCP and CSD rules and of the Code of Practice for RPSOs and SSPs, as described in Section 3 of this supervisory statement. The Bank would expect an FMI to submit a report within 24 hours of determining an operational incident has met a threshold. The Bank acknowledges that where an operational incident requires all the FMI's resources to address the incident, the FMI may take longer than 24 hours to submit a report.

4.5 An FMI should balance the need to submit an incident report to the regulators with prioritising the necessary actions to resolve and recover from the operational incident.

Intermediate operational incident report

4.6 The Notifications and Regulatory Reporting Parts of the of the CCP and CSD rules and of the Code of Practice for RPSOs and SSPs require an FMI to submit an intermediate report as soon as practicable after there has been a significant change in circumstances from that described in the last incident report submitted by the FMI. Under Rule 4.2 of the CCP and CSD rules and of the Code of Practice for RPSOs and SSPs, FMIs are required to submit one or more intermediate reports to keep the regulators informed of any significant changes to an operational incident in a timely manner and provide further details on the incident as well as any actions the FMI is taking to resolve/remediate the impact of it.

4.7 A significant change in the incident could include a change in impact or the status of the incident. Examples of where FMIs should submit an intermediate report include, but are not limited to:

- The FMI identifying the origin of, or becoming aware of further information related to, the incident.

- The impact of an operational incident becoming more severe.
- The activation of a business continuity plan, disaster recovery plan or significant changes to the resolution strategy of the operational incident.
- The FMI resolving the operational incident.

4.8 As set out above, an FMI is required to submit an intermediate report each time a significant change occurs. This means that FMIs may be required to submit multiple intermediate reports. At least one intermediate report is required to inform the Bank once the FMI has resolved the operational incident.

4.9 An FMI should balance the need to submit an incident report to the regulators with prioritising the necessary actions to resolve and recover from the operational incident.

4.10 In the event that an FMI has resolved an operational incident prior to submitting an initial report, they are not required to complete an intermediate report and can move straight to the final report stage.

Final operational incident report

4.11 Once an operational incident has been resolved, an FMI must submit a final report to the Bank within 30 working days after the operational incident has been resolved or, where this is not practicable, as soon as is practicable but not exceeding 60 days.

4.12 The Bank expects an FMI to submit an incident report within 30 working days unless there are circumstances which would necessitate further time to collect all the information required in the final report. This could include, but is not limited to, where an incident is of such complexity that further time is required to substantiate the root cause of an incident, or where an FMI is reliant on another party to complete the necessary information, such as a third party.

4.13 FMIs are expected to inform the Bank when it is impracticable to submit the final report within 30 working days, explaining the reason as to why it is impracticable and the expected timeframe for the submission of the final report.

Appendix 4: Draft amendments to the outsourcing and third-party risk management supervisory statement for CCPs

[Draft amendments to the outsourcing and third-party risk management supervisory statement for CCPs](#) 

Appendix 5: Draft amendments to the outsourcing and third-party risk management supervisory statement for CSDs

[Draft amendments to the outsourcing and third-party risk management supervisory](#)

[statement for CSDs](#) 

Appendix 6: Draft amendments to the outsourcing and third-party risk management supervisory statement for RPSOs and SSPs

[Draft amendments to the outsourcing and third-party risk management supervisory statement for RPSOs and SSPs](#) 

Appendix 7: Cost benefit analysis

1: Introduction

1 The Financial Services and Markets Act 2000 (FSMA), as amended, requires the Bank to publish a cost benefit analysis (CBA) of proposed rules for central counterparties (CCPs) and central securities depositories (CSDs).[10] This is defined as ‘an analysis of the costs, together with an analysis of the benefits that will arise if the proposed rules are made’.[11]

2 FSMA 2000 requires regulators to provide an estimate of the costs and benefits of the proposals, unless, if in the opinion of the regulators, the costs and benefits cannot reasonably be estimated or it is not reasonably practicable to do so.[12] Where estimates cannot be ascribed a monetary value, other estimates of outcomes are provided.

3 The analysis has been conducted with regard to the Bank’s primary objective to protect and enhance the stability of the UK financial system (the Financial Stability Objective), and the Bank’s secondary objective to, where possible, facilitate innovation in the provision of CCP and CSD services when advancing the primary financial stability objective (the Secondary Innovation Objective). Although the CBA requirement does not apply to the Bank’s power to publish binding Codes of Practice for recognised payment system operators (RPSOs) and specified service providers (SSPs) under the Banking Act 2009, the Bank has carried out a proportionate CBA in respect of the proposed Code of Practice for payment systems.

4 The Bank is consulting on proposals for incident and outsourcing and third-party reporting (IOREP). It consists of three main proposals relating to incident reporting, material third-party (MTP) arrangements notifications, and the MTP Register. IOREP has been developed jointly with the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA).

5 The Bank has consulted the CBA Panel (‘the Panel’) on the preparation of this CBA. The Bank submitted a draft CBA for the Panel to review prior to a meeting to discuss its feedback and advice. The Panel provided feedback on the way the draft CBA addressed the analysis of the proposals’ counterfactual; the average ongoing costs of some proposals; and the analysis of the proposals’ positive benefits. In summary:

- the Panel advised further detail be provided on the benefits of the policy. The Panel

recommended to more explicitly express that a key benefit of the proposals would be to better identify concentration risks within the sector, and add further detail on the proposed actions and the data that demonstrates how these benefits are realised. Paragraphs 47 to 50 have been amended to add that information collected could help the Bank to better identify concentration risk, and note that aggregated anonymised trends would enable the Bank to work with FMIs to prioritise the mitigation of incident impacts and potential key vulnerabilities. The Bank has also added in further text on the potential costs of operational incidents, which are occurrences the Bank seeks to limit through using the data it is proposing to collect.

- the Panel recommended the Bank to further clarify the analysis of the proposals' counterfactual, for example how limiting existing data collections to material outsourcing arrangements could limit the Bank's oversight of sector-wide risk. Paragraph 12 has been amended to develop this analysis.
- the Panel queried the average ongoing cost per firm to maintain the material third-party register annually. Paragraph 40 confirms that these estimates are derived as a simple average across the population of in-scope FMIs, and Paragraph 3.21 of the main consultation paper clarifies the proposed requirements for maintaining the material third-party register.

Case for regulatory intervention

6 The full case for regulatory intervention is set out in Section 1 of the consultation paper.

7 A key priority for the Bank is to put in place a stronger framework for the supervision of individual FMIs and wider financial sector operational resilience, following the publication of the Bank's [policy on Operational Resilience of FMIs](#) in March 2021. As part of that framework, the Bank has previously publicly committed to consider regulatory reporting requirements for operational incidents.^[13]

8 In 2019, the Treasury Select Committee published a [report examining the 2018 IT failures in the UK financial services sector](#)^[14]. This report made several recommendations for regulators, including assessing the accuracy and consistency of incident reporting data, clarify standards, guidance and definitions for industry and considering the need to expand reporting requirements.

9 In 2024, the Bank published its final policy statement on a new regulatory regime for Critical Third Parties (CTPs) to the financial sector in [PS16/24 – Operational resilience: Critical third parties to the UK financial sector](#). PS16/24 recognises the risk that severe disruption arising from certain third parties could pose to the safety and soundness of FMIs, policyholder protection, and the financial stability of the UK. To support the identification of potential CTPs and assess where critical nodes of failure could arise, the Bank needs to collect adequate data on FMIs' MTP arrangements.

10 The Bank currently faces challenges in assessing risks to its objectives and, where appropriate, acting when operational disruption occurs. The Bank collects data on operational

incidents and MTP arrangements in an unstructured manner under existing requirements and expectations.

11 The proposals in the CP aim to ensure that FMIs submit consistent and good-quality reporting of operational incidents and material third-party arrangements by:

- **Prioritising the most significant risks to operational resilience:** by setting out clear requirements which enable FMIs to prioritise the reporting of operational incidents and MTP arrangements to those which could pose risks to the delivery of an important business service (IBS), or to the financial stability of the UK.
- **Setting out standardised reporting requirements:** to enhance the quality and comparability of information submitted to the Bank on operational incidents and MTP arrangements. This would make reporting processes more efficient for FMIs, allow the Bank to understand potential risks and vulnerabilities within the financial sector more efficiently, and better identify FMIs' reliance on material third parties.

12 The counterfactual of the proposals is that the Bank continues to collect information under existing requirements and expectations. However, this may mean that the Bank continues to collect this in an unstructured manner, which could lead to the Bank inefficiently monitoring FMIs' and the financial sector's operational resilience and systemic concentration risk arising from FMIs' use of third parties.

Baseline and key assumptions

Baseline

13 The Bank has estimated the additional costs above the baseline, reflecting the incremental changes that FMIs would not have undertaken in the absence of the regulations. The estimates in this CBA therefore makes the following baseline considerations.

14 FMIs already incur information gathering costs associated with the IOREP proposals. In complying with the requirements set out in Rule 4 of the Recognised Clearing House Instrument 2018, the onshored version of the EU Central Securities Depositories Regulation (909/2014) (UK CSDR) and pursuant to firm-specific notices issued by the Bank under the Banking Act 2009, Section 204), the Bank considers that UK FMIs are already collecting data on relevant operational incidents and have been notifying some of these details to the Bank.

15 FMIs have been increasingly reliant on third-party providers to support the delivery of business operations. It is possible that following the introduction of these proposals that reporting increases further to reflect this trend, but it is not possible to accurately predict this.

Key assumptions

16 The estimates in this CBA are indicative and rely on key assumptions based on available

historical data.

17 FMI report in different frequencies due to individual FMI differences. Historical reporting data suggests that not all FMIs in scope would experience an operational incident or change or enter into a MTP arrangement in a given year. FMIs may also have different interpretations of the reporting materiality thresholds which could influence their reporting frequency. As a result, some FMIs may submit more reports than other FMIs under the proposed requirements.


Summary of benefits and costs

18 The sections below assess the one-off and ongoing (annual) costs and benefits arising from the proposals. Based on the analysis of costs and benefits of the proposals that are set out below, the Bank expects that the proposals would bring net benefits to the UK financial sector.

19 The costs include compliance costs to FMIs directly arising from the proposals, which are additional above the baseline as outlined above. Table A summarises the estimated upper bound of average costs across all FMIs in scope of the proposals.

Table A: Estimated one-off and ongoing (annual) aggregate costs to all FMIs in scope

Cost type	Estimated cost (£)	
	CCPs and CSDs	RSPOs and SSPs
Total one-off costs	106,500	164,000
Total ongoing costs	41,000	38,500
Total Present Value of all costs	459,000	493,000

Note: A Present Value is the sum of all one-off and ongoing costs over 10 years, discounted to today using a discount rate of 3.5% in line with the approach set out in the [HM Treasury Green Book \(2022\)](#) .

20 The benefits from the proposals are expected to arise through enhanced visibility of individual FMIs' and broader financial sector operational resilience and systemic concentration risk arising from FMIs' use of third parties. Where appropriate, the Bank may use the data and share aggregated anonymised trends to work with FMIs to prioritise the mitigation of incident impacts and potential key vulnerabilities. This should reduce the likelihood of major disruption occurring, which imposes costs on both FMIs and the broader financial system. The introduction of standardised reporting guidance could also provide ongoing efficiency gains for FMIs. The Bank may also use the information to inform the identification of potential candidates to recommend to HM Treasury as Critical Third Parties to the UK financial sector. The indirect benefits of the proposals could include the maintenance of trust and confidence in the Bank's regulatory

framework, supporting FMI's ability to innovate within this framework.

21 The Bank has concluded that the proposals are likely to bring net benefits to the financial sector. While there are costs associated with the implementation and ongoing compliance with the proposals, the Bank considers that improved oversight of risks to FMI's operational resilience can lead to the maintenance of confidence in the financial sector and trust in the Bank's regulatory framework.

Affected FMI population

22 The IOREP proposals affect 10 FMI's, consisting of three UK recognised CCPs, one recognised UK CSD, five UK RPSOs and one UK SSP.

23 For the purposes of the CBA, the FMI's are divided into two groups: (1) CCPs and CSDs and (2) RPSOs and SSPs. We assumed that all FMI's are of a similar large size to allow for a conservative estimate of one-off implementation and ongoing compliance costs.

2: Costs of the proposals

Costs to FMI's

24 The Bank is proposing to introduce new reporting requirements to collect structured information on FMI's operational incidents and MTP arrangements. The proposals are summarised in Table B below, and details can be found in the main paper.

Table B: Summary of the IOREP proposals


Proposal	Incident reporting	MTP notifications	MTP register
Proposed requirements	Submit structured information on operational incidents	Submit structured information on new MTP arrangements or significant changes to existing individual MTP arrangements	Submit database of aggregated MTP arrangements
Submission method	FCA Platforms	Electronic means	FCA Platforms
Materiality thresholds	Operational incidents which could pose a risk which could disrupt the FMIs provision of an important business service for a prolonged period; or otherwise pose a risk to the stability of the UK financial system	All MTP arrangements	All MTP arrangements
New or amendments to existing requirements?	New requirements (additional to existing requirements)	New requirements (additional to existing requirements and expectations)	New requirements (additional to existing requirements and expectations)

25 The Bank expects that there would be one-off costs to FMIs to familiarise themselves with the proposals and set-up costs associated specifically with the creation of a MTP register. There would also be annual ongoing costs to FMIs to comply with the proposed requirements, which would arise when an FMI experiences an operational incident or enters into or changes a MTP arrangement that meets the reporting materiality thresholds.

26 As outlined in Section 1, the estimates of annual ongoing costs are underpinned by the key assumption that FMIs would submit reports or make changes to MTP registers in different frequencies.

27 The data sources used to estimate these costs are set out below, followed by the analysis of the estimated costs of each of the three proposals to FMIs.

Data

28 The Bank used a range of sources to estimate the likely costs to FMIs from the proposals. This includes responses to a Bank request for information shared with all relevant FMIs, historical reporting data, and outputs from [the FCA's Standardised Cost Model](#) .

29 The Bank estimated the incremental costs to FMIs primarily using FMIs' responses to its request for information. FMIs were asked to estimate the average full-time equivalent (FTE) effort to comply with existing processes, which are used as a proxy to estimate the potential costs of the IOREP proposals. This includes the estimated average FTE effort costs of completing an operational incident report or MTP notification template each time an operational incident occurs, or an FMI enters into or significantly changes an MTP arrangement.

30 The estimates FMIs provided are based on each individual instance of a FMI needing to submit an operational incident report or MTP notification, or amend its MTP register. To calculate the annual ongoing cost, the Bank applied a probability that an FMI would submit a report as informed by historical reporting data. This reflects the key assumption outlined above that not all FMIs would incur compliance costs associated with all IOREP proposals each year.

31 The Bank translated the estimated average annual ongoing FTE effort costs into monetary values by making use of compensation figures available from the Robert Walters (2023) survey data.

32 The FCA's Standardised Cost Model was used to estimate one-off compliance costs relating to familiarisation and gap analysis associated with the proposals. The model calculates the one-off familiarisation and gap analysis costs for FMIs based on the length of publications, such as consultation papers, and the length of legal instruments respectively. The model assumes that costs occur to firms according to their size in the SCM, as defined using FCA fee-block data.

Uncertainties in the data

33 The CBA estimates are subject to several uncertainties. For example, in its request for information, the Bank asked FMIs to estimate a range of costs based on compliance with existing requirements and their own internal processes, which may not map exactly to the proposed IOREP requirements.

34 The use of Bank historical reporting data to estimate reporting volumes is also subject to the caveat that due to the unstructured nature of the data currently collected, the estimated reporting volumes should be treated as a rough estimation of actual volumes.

One-off costs

35 FMIs are expected to incur one-off costs to familiarise themselves with the proposals and conduct a gap analysis of the new requirements against current practices to understand the changes they would need to implement to meet the requirements. The amount of time required for

each FMI would depend on the nature, scale and complexity of each FMI.

36 FMIs would also incur additional costs of setting up and submitting an MTP register for the first time. While the proposals would not require FMIs to build technology infrastructure to submit the MTP register, the Bank recognises that FMIs may want to do so in future for efficiency. The total estimated one-off FTE effort therefore includes both staff time and technology build cost to complete the MTP register. The average one-off FTE effort to set up the MTP register for an individual FMI is c.32 FTE days.

37 The Bank's estimates of the MTP register set-up costs should be considered an upper bound estimate, as they assumed that all FMIs will need to create a new MTP register having not completed one previously. However, the Bank recognises that most FMIs in scope (80% of the population) already have at least a register of material outsourcing arrangements and therefore would incur lower costs to adapt to the new proposed requirements.

38 The Bank used outputs from the FCA's SCM to estimate the cost to FMIs to familiarise themselves with the proposals and complete gap analysis. To estimate the one-off costs to comply with the MTP register requirements, the Bank added these familiarisation costs to the estimates of set-up costs provided by firms in their response to its request for information.

39 Table C summarises the estimated operational one-off compliance costs to industry associated with each of the proposals. The FCA's SCM produces structured outputs as central estimates, whereas the data derived from the Bank's request for information was largely unstructured. The Bank used upper-bound responses from the latter in order to ensure conservative cost estimates.

Table C: Estimated one-off compliance costs associated with IOREP proposals, by FMI group (£)

Firm type/proposal	Per CCP/CSD	CCP and CSD industry	Per RPSO/SSP	RPSO and SSP industry
Operational incident reporting	Central estimate			
	1,470	5,880	1,470	8,820
MTP Notifications	Central estimate			
	580	2,320	580	3,480
MTP Register (includes central estimate)	24,512	98,047	25,236	151,414

Ongoing compliance costs

40 An individual FMI in scope is expected to incur ongoing compliance costs each time it needs to submit an operational incident report, MTP notification, or to update its MTP register. The (annual) frequency of reporting would depend on its individual business model as assumed above. Therefore, the Bank does not expect that all FMIs in scope would submit an operational incident report or MTP notification, or update its MTP register, each year.

41 Using historical reporting data and FMIs' responses to the Bank's request for information, the Bank estimated the average probability of a FMI submitting a report or updating its MTP register in a given year, alongside the average FTE effort days to undertake this. In summary, the Bank estimates that on average:

- an individual CCP/CSD will experience c.1.7 reportable operational incidents per year, and would take c.5 FTE days to complete an individual report;
- an individual RPSO/SSP faces a probability of 56% per year that it would experience a reportable operational incident, and would take c.2 FTE days to complete an individual report;
- an individual CCP/CSD will notify the Bank 1.7 times per year of a new or change to a MTP arrangement, and would take c.3 FTE days to complete an individual MTP notification;
- an individual RPSO/SSP faces a probability of 41% per year that it would need to notify the Bank of a new or change to a MTP arrangement, and would take c.2 FTE days to complete an individual MTP notification;
- an individual CCP/CSD will make 3.4 changes to the MTP register per year, and would take c.7 FTE days to undertake the update; and
- an individual RPSO/SSP will make 0.8 changes to the MTP register per year, and would take c.5 FTE days to undertake the update.

42 The ongoing costs primarily arise from FMIs completing a template for incident reporting or MTP notifications, or updating the MTP register. Table D summarises the ongoing (annual) costs of compliance, considering the estimated probability of reporting and frequency of changing a MTP register.

Table D: Average ongoing (annual) operational compliance costs associated with IOREP proposals, by FMI group (£)

Firm type/proposal	Per CCP/CSD	CCP and CSD industry	Per RPSO/SSP	RPSO and SSP industry
Incident reporting	3,574	14,296	1,609	9,652
MTP Notifications	1,873	7,494	1,469	8,816
MTP register	4,802	19,210	3,298	19,791

Costs to FMIs' participants

43 This policy does not impose a direct cost on FMIs' participants. However, FMIs may choose to cover the costs of the policy through use of retained profits, decreasing their current profits, or increasing fees to their participants for using their services. This decision will be distinct for each FMI. As such it would not be reasonably practicable for the Bank to estimate how these costs may fall.

Costs to the Bank

44 There would be additional costs to the Bank for supervising against the proposed rules and expectations on operational incident reporting, notifications and the MTP register. However, the Bank considers these costs to be minimal. Supervisory time and technology resource will be required to review and analyse the data received from incident reports and the MTP register, but the standardisation of templates and the use of a reporting solution is expected to offset the costs for data processing and analysis.

45 There may also be additional costs to the Bank associated with FMIs using the FCA platforms to submit incident reporting data and the material third-party arrangement register to the Bank, should these platforms be used. However, these are likely to be minimal because the Bank will be sharing use of the portal for this purpose with the PRA and FCA.

3: Benefits of the proposals

46 The Bank expects that several benefits would emerge as a result of the IOREP proposals. The key mechanisms from which these benefits are expected to materialise are through improved visibility of operational resilience of FMIs, and the wider financial sector, and of systemic concentration risk arising from FMIs' use of third parties.

Improved oversight of sector-wide operational resilience

47 The Bank considers that the financial sector would benefit from improved oversight of individual FMI and sector-wide operational resilience and systemic concentration risk arising from FMIs' use of third parties. This is facilitated by the collection of structured data, which would improve the quality of the Bank's existing understanding of these risks.

48 The Bank would use this data to identify efficiently third parties who could be critical to the financial sector. The Bank can recommend these third parties to be designated as critical to HM Treasury, and be brought into scope of the Bank's new supervisory oversight regime. This can result in further indirect benefits materialising to the operational resilience of the sector, as outlined in the CBA associated with **CP26/23 – Operational resilience: Critical third parties to the UK financial sector**.

49 In collecting standardised data on operational incidents and MTP arrangements, the Bank can better identify emerging trends and vulnerabilities at individual FMIs and the sector. For example, where an operational incident originates at a third party used by multiple FMIs the Bank could, where appropriate, proactively reach out to FMIs in instances where other FMIs may be unaware of the issue. Where appropriate, the Bank could also provide feedback to individual FMIs or share anonymised aggregated trends with industry on the emerging risks.

50 While it is not possible for the policy proposals to completely mitigate the possibility of major incidents, better data can enable the Bank to work with FMIs to address outstanding vulnerabilities and reduce loss^[14] from operational disruption. This should reduce the likelihood of major disruption occurring. An indicative example of the possible impact of disruption is the partial service disruption at Visa Europe in 2018, which led to 5.2 million debit and credit card transactions being disrupted over a 10-hour period, directly impacting trust in the UK financial sector causing wider implications to firms and FMIs and the wider UK economy.^[15] Another indicative example is the system outage to its settlement system for securities transactions experienced by UK CSD EUI (Euroclear UK and International), which caused notable market disruption. The disruption was due to the messaging software component of the CSD's operations.

51 The proposals also seek to collect information on FMIs' compliance with existing operational resilience and outsourcing and third-party risk management requirements and expectations. Structured data enables the Bank to provide constructive feedback to FMIs to address potential gaps and strengthen their overall risk management.

Efficiency gains from clearer reporting requirements

52 The proposals could lead to efficiency gains for FMIs. Clear guidance on reportable operational incidents and MTP arrangements, thresholds and information required for submission to the regulator would improve efficiency of reporting and decrease resourcing and costs to FMIs over time. The improved reporting clarity could reduce iterative exchanges with the Bank, particularly during time-sensitive disruptions. The formalisation of MTP register expectations into

rules would also provide greater regulatory clarity for FMIs.

53 The Bank has also sought to limit costs for FMIs by targeting the collection of data to the minimum information that the Bank would require to ensure effective oversight of sector-wide operational resilience. This arises through the setting of reporting thresholds and limiting the proposed data fields featuring in the structured reporting templates.

54 The proposed approach is aligned between the Bank, PRA and FCA. The supervisory authorities are proposing to provide a shared reporting approach and reporting technology solution, which could minimise reporting burden and complexities.

55 Based on high-level insights from the **Transforming Data Collection** Industry Cost Survey, factors such as greater clarity and consistency in reporting requirements across collections combined with a technology solution could potentially result in cost savings in the order of 10% of FMIs' overall ongoing reporting costs. Having considered these insights, the incremental ongoing reporting costs to FMIs as a result of the IOREP proposals could be limited as the Bank is proposing to introduce clear guidance and a simplified reporting solution for IOREP.

Appendix 8: Incident reporting fields template

Incident reporting fields template

Appendix 9: Material third-parties reporting fields template

Material third-parties reporting fields template

-
1. Schedule 17A of FSMA 2000 as amended by FSMA 2023.
 2. **Transforming data collection: Bank of England and FCA deliver on phase one commitments – 6 July 2023.**
 3. The Bank sets out its approach to identifying potential CTPs and recommending them to HMT for designation in **PS16/24 – Operational resilience: Critical third parties to the UK financial sector.**
 4. The information the Bank requires from RPSOs/SSPs pursuant to firm-specific notices issued by FMID under s204 (information requirements) of the Banking Act 2009.
 5. **Fundamental Rules for financial market infrastructures.**
 6. In carrying out policymaking functions the Bank is required to comply with several statutory obligations. This section explains how the Bank has had regard to the obligations applicable to the Bank's policy development process, including an explanation of how this is reflected in the proposals.
 7. **Joint foreword: Critical third parties to the UK financial sector.**
 8. In line with the FSB's – Enhancing Third-Party Risk Management and Oversight, an nth-party is a service provider that is part of a third-party service provider's supply chain and supports the ultimate delivery of services to one or more

financial institutions.

9. [Financial Services and Markets Act 2023](#), section 48; [Bank of England Act 1998](#) sections 30D, 30E, 30I.
10. In accordance with s.138JA (1) FSMA 2023 as applied to the Bank by paragraphs 10(1) and 10A of Schedule 17A.
11. s.138J(7) FSMA 2000.
12. s.138J(8) FSMA 2000.
13. [Transforming data collection: Bank of England and FCA deliver on phase one commitments – 6 July 2023](#).
14. The FCA calculated the average cost per incident at FMIs as £786,000 (in 2024 terms) in its [CP19/32 – Building operational resilience](#).
15. [Visa's response on its system failure published](#), UK Parliament.