FINANCIAL CONDUCT AUTHORITY

Consultation Paper

CP24/28**

Operational Incident and Third Party Reporting

December 2024

How to respond

We are asking for comments on this Consultation Paper (CP) by **Thursday 13 March 2025**.

You can send them to us by responding to the email address below.

Or in writing to:

Technology, Resilience & Cyber Department
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Email:
cp24-28@fca.org.uk

Sign up for our **news and publications alerts**

See all our latest press releases, consultations and speeches.

Disclaimer

When we make rules, we are required to publish:

- a list of the names of respondents who made representations where those respondents consented to the publication of their names,
- an account of the representations we receive, and
- an account of how we have responded to the representations.

In your response, please indicate:

- if you consent to the publication of your name. If you are replying from an organisation, we will assume that the respondent is the organisation and will publish that name, unless you indicate that you are responding in an individual capacity (in which case, we will publish your name),
- if you wish your response to be treated as confidential. We will have regard to this indication, but may not be able to maintain confidentiality where we are subject to a legal duty to publish or disclose the information in question.

We may be required to publish or disclose information, including confidential information, such as your name and the contents of your response if required to do so by law, for example under the Freedom of Information Act 2000, or in the discharge or our functions. Please note that we will not regard a standard confidentiality statement in an email message as a request for non-disclosure.

Irrespective of whether you indicate that your response should be treated as confidential, we are obliged to publish an account of all the representations we receive when we make the rules.

Further information on about the FCA's use of personal data can be found on the FCA website at: www.fca.org.uk/privacy.

Contents

Chapter 1

Summary

Why we are consulting

1.1 Financial services firms face growing challenges to remaining operationally resilient. When operational incidents do occur, the disruption to firms' services can harm consumers and the wider sector. As part of our strategic commitment to minimise the impact of these operational disruptions, we are consulting on a new approach for firms to report incidents to us. This will help us to respond to those incidents, to understand their impact and the steps firms are taking both individually and across the sector.

1.2 Currently, feedback from industry shows that some firms are unclear on how and when to inform us about operational incidents. By proposing clearer definitions of what constitutes an 'operational incident', when these should be reported, and a standardised template, this will set clearer expectations and ensure a level playing field for firms to operate within.

1.3 We also want to have a better understanding of firms' important third party suppliers (material third parties) and collect information on these arrangements in a more structured manner. This will help us to respond more quickly and effectively to incidents related to third parties, which will in turn benefit firms and the financial sector. This is important as firms are increasingly reliant on third party services to help run their operations. Additionally, this information will help us to understand where firms rely on the same third parties. This will support the identification of potential critical third parties (CTPs) which we will recommend to HM Treasury to consider for designation under the CTP oversight regime.

1.4 We propose to apply the material third party reporting requirements to a smaller sub-set of firms (set out in 1.7) whose services, if disrupted, could have significant consumer or market impact.

1.5 Our proposals, developed with the Prudential Regulation Authority (PRA) and the Bank of England (the Bank), aim to enhance incident and third party risk management, strengthen firms' operational resilience, and minimise harm.

Who this applies to

1.6 Chapter 3 of this CP, which covers proposals for operational incident reporting, is relevant to:

- a firm
- a payment service provider
- a UK Recognised Investment Exchange (RIE)
- a registered trade repository
- a registered credit rating agency

1.7 Chapter 4 of this CP, which covers proposals for third party reporting, is relevant to a firm that is:

- an enhanced scope Senior Managers & Certification Regime (SM&CR) firm
- a bank
- a PRA designated investment firm
- a building society
- a Solvency II firm
- a Client Assets Sourcebook (CASS) large firm
- a UK recognised investment exchange (RIE)
- an authorised electronic money institution or an authorised payment institution
- a consolidated tape provider

1.8 Consumers may be interested in how operational resilience is being improved within firms.

Measuring success

1.9 We expect to receive more detailed, accurate and consistent data from firms through our proposed data returns for both incidents and material third party arrangements. This should enable us to better understand the operational resilience of individual firms and the wider financial services sector. It will allow us to respond to incidents more efficiently, and identify where the financial sector has an over-reliance on certain third party services. The latter will support us in collecting the relevant data to identify third parties for HM Treasury to consider for designation under the CTP regime, aimed to reduce systemic third party risk to UK's financial system.

1.10 To measure our success, we will consider:

- the timelines of the operational incidents reported to us, the accuracy of information provided, the usefulness of the information to manage the incident, and the time taken to confirm the root cause of an incident
- the identification of thematic insights from both incident and material third party reporting that enables supervisors to take early intervention, in turn protecting consumers and the market from disruption
- the timely identification of concentration in third parties servicing firms that pose systemic risk to the UK's financial system

Next steps

1.11 We want to know what you think of our proposals. Send us your comments by Thursday 13 March 2025.

1.12 Use the response form on our website, email us at cp24-28@fca.org.uk or write to us at the address on page 2.

1.13 We will consider all feedback and publish our finalised rules in a Policy Statement (PS) next year in H2 2025.

Chapter 2

The wider context

The harm we are trying to reduce/prevent

2.1 Consumers and markets rely on financial services to be resilient, and we want to understand more about operational incidents to address the limitations in the information we currently receive about them. However:

- Feedback from industry, as part of the Transforming Data Collection programme in 2022, showed that some firms are unclear on how and when to inform us about incidents.
- Since 2018, over 20% of operational incident reports submitted by firms arrived over 11 days after the incident began.
- Since 2018, approx. 2 to 2.5% of regulated firms reported an operational incident to us, which may indicate significant underreporting of incidents.
- Currently, there is no template for firms to report incidents, so the information we receive from incident notifications is inconsistent. This makes it harder for us to promptly review and respond to individual incidents, and to understand links between them. It also hinders our ability to properly analyse notifications and draw out thematic observations to feed back to the industry.

2.2 These limitations make it more difficult for the regulators to work with firms to effectively manage the impact of incidents. This increases the possibility of disruption to firms, markets, and result in harm to consumers.

2.3 To address this, we are proposing clear definitions of what constitutes an 'operational incident' and when to report one. We also propose a standardised incident reporting process and template.

2.4 To improve our visibility, and in line with international expectations, we propose to require firms to collect and periodically submit information on an expanded range of material third party arrangements. Receiving this information in a structured way will make it easier for us to understand and respond to the risks in third party arrangements at individual firms and the systemic risks where many firms rely on the same third party. For a smaller sub-set of firms (as set out in 1.7), we are proposing to:

- expand the scope of existing outsourcing notifications, covering both material outsourcing and material non-outsourcing arrangements (collectively referred to as 'material third party arrangements') for in-scope firms
- provide a template for firms to submit notifications of new third party arrangements, or changes to existing arrangements
- require firms to maintain and submit a register of these arrangements to us, ensuring this is updated annually

2.5 As firms increasingly rely on third parties for a range of their services, operations and activities, the distinction between outsourcing and non-outsourcing third party arrangements is no longer relevant when considering a firm's third party risks. 'Outsourcing' is when a firm arranges for a service provider to perform a process, service or activity on its behalf that the firm would otherwise have carried out itself. However, third parties can also provide services that are not classed as outsourcing, and this is what we refer to in this CP as 'non-outsourcing'. It is important for us to have visibility of all 'material third party arrangements' because both types – outsourcing and non-outsourcing – can cause serious incidents at firms and across the sector. This has also been recognised internationally. For example the Financial Stability Board published a toolkit in 2023 to address all third party-related risks and not just risks related to outsourcing.

How it links to our objectives

Consumer protection

2.6 Providing clarity on when, how, and which operational incidents firms should report to us will help us engage with firms in a more timely and effective manner, and better understand the consumer impact. Collecting structured data on firms' third party arrangements will help us to identify risks that may affect consumers. This will enable us to engage earlier with firms to manage these risks appropriately.

Market integrity

2.7 Operational disruptions pose risks to the soundness, stability and resilience of the UK financial system and the orderly operation of financial markets. Providing clarity on when, how, and which operational incidents firms should report to us will help us identify threats to market confidence. This will enable us to engage with firms early on, so they appropriately respond to such incidents helping to minimise market disruption.

2.8 Collecting structured data on firms' third party arrangements will support our identification of potential critical third parties (CTPs) that, if disrupted, could threaten the stability of, or confidence in the UK financial system. Should HM Treasury designate these third parties as 'critical' under the CTP oversight regime, the oversight of such systemic third parties will protect and enhance the integrity of the UK financial system will promote market stability.

Competition

2.9 Resilient firms can promote effective competition. We will help promote effective competition by empowering consumers to make more informed choices on what services to use, from a wider population of more resilient firms. This may drive firms to improve their operational resilience as one way to compete for, and keep, clients. We will do this by collecting consistent and structured data on both operational incidents and third party concentration risk, to identify and share insights from this data with industry and to work with industry to improve the sector's overall operational resilience.

Secondary international competitiveness and growth objective (SICGO)

2.10 To reduce reporting complexities and advance our policy aims, we have aligned these proposals to similar international incident and third party reporting frameworks, such as the Format for Incident Reporting Exchange (FIRE) from the Financial Stability Board (FSB), and the European Union's (EU) Digital Operational Resilience Act (DORA).

2.11 We have developed our proposals to help strengthen incident and third party risk management, and enhance both firms and the wider sector's operational resilience. We believe these proposals will advance the SICGO objective by contributing, financial stability, making the UK a more attractive place to do business and enhance its competitiveness.

Wider effects of this consultation

2.12 This work has been undertaken as part of our long-term prioritisation of firm resilience and our strategic commitment to minimise the impact of operational disruptions.

2.13 We apply our proposals proportionately to firms by setting reporting thresholds, making it clearer for firms or markets when they need to report an incident. Not all incidents impact firms in the same way, and firms will be asked to consider various factors when assessing if an incident needs to be reported. This includes a firm's position and size in the market they operate in, their business model and client base. Equally, and using the information that we propose to receive, we will be proportionate in our response to the incidents that reported to us.

2.14 For reporting on third party arrangements, we apply our proposals proportionately by only collecting information on third party arrangements that are material. Additionally, these proposed requirements are limited to mainly firms in scope of SYSC 15A Operational resilience.

Cost benefit analysis

2.15 The Financial Services and Markets Act (2000) requires us to publish a cost benefit analysis (CBA) of our proposed rules. Specifically, section 138I requires us to publish a CBA of proposed rules, defined as 'an analysis of the costs, together with an analysis of the benefits that will arise if the proposed rules are made'. The full cost benefit analysis is set out in Annex 2.

2.16 The CBA assesses the one-off and ongoing (annual) costs and benefits arising from the proposals. Based on the analysis of the costs and benefits of the proposals, we expect that the proposals would bring net benefits to the UK financial sector. The estimated costs and benefits are summarised below.

2.17 Consumers and market participants will indirectly benefit from improved incident reporting because we will be able to act sooner in the event of operational incidents and

third party disruptions to minimise harm. A register of third party arrangements will also enable us to identify third party concentration risks quicker, by identifying other firms affected by incidents using the submitted register data. We may also be able to use the incident and third party data to enable future work seeking to prevent consumer harm and market disruption from incidents.

2.18 The scale of losses caused by incidents can be large. Therefore, any small improvement to the reporting process could help to offset the costs to firms to report to us, whether the improvements allow us to monitor market-wide risks better or simply allow us to support firms to manage incidents faster.

2.19 The one-off costs of the Operational Incident Reporting and Third Party proposals are estimated to be between £19.14 and £26.71 million and the ongoing (annual) costs are £0.04 to £0.12 million. These are expected to be offset annually by an estimated £0.27 million in efficiencies to firms and non-quantified benefits to the market through minimising harm from incidents and third party risks.

2.20 Firms will also benefit from the new standardised incident reporting proposal. The Handbook will be updated to give more clarity over what and when to report to us, and the use of our template to submit information will reduce uncertainty over what information is required in an incident notification.

2.21 Firms and the FCA are both expected to save some time spent in follow-up after an incident notification is submitted, as the new template will ensure the necessary information is provided through the initial notification. We estimate annual efficiencies to be approximately £0.27 million to firms based on estimates from our supervisory insight, firm outreach by the regulators, and the rate of incident notifications. As firms will need to adjust to the new reporting process, we estimate these efficiencies may be offset in year one of the proposals.

2.22 Firms will face costs to comply with our proposals. The one-off costs of the incident reporting and third party proposals are estimated to be between £19.14 and £26.71 million and the ongoing (annual) costs are £0.04 to £0.12 million. We assume that firms will incur one-off costs to familiarise themselves with the proposals and perform gap analysis, particularly around non-outsourcing third parties. Once familiar, we expect no further new ongoing costs for the incident reporting proposals as firms currently report incidents to us. For the third party reporting proposal, we expect there is a one-off cost to set up a register using our template and an ongoing cost to update it annually, estimated using firms' responses to PRA firm outreach. However, firms should have the information required on their material non-outsourcing arrangements in line with SYSC 15A where firms are expected to understand the third party arrangements supporting their important business services.

2.23 Consumers and market participants will indirectly benefit from improved incident reporting because we will be able to act sooner in the event of material incidents and third party disruptions to minimise harm. We may also be able to use the data gathered to enable future work seeking to prevent consumer harm and market disruption. Therefore, any small improvement to the reporting process could help to offset the costs, whether the improvements allow us to monitor market-wide risks better or simply allow us to support firms to manage incidents faster. We assume firms will need to

familiarise themselves with the new notification template and perform a gap analysis. These are one-off costs and are estimated using our standardised cost model (SCM). Once firms are familiar with the new process, we assume that there are no new ongoing costs above the existing process of reporting incidents.

2.24 Firms and the FCA are both expected to save some time spent in follow-up after a notification is submitted, as it will contain the necessary information, so further information gathering will not be needed. These efficiencies are quantified using estimates from our supervisory insight, and firm outreach by the FCA and the PRA. As firms will need to adjust to using the new template, we estimate these efficiencies may be offset in year one.

2.25 The third party proposals require annual submission of a register to us. This will enable us to identify third party risks and incidents quicker, by identifying other affected firms using the submitted register data. In addition to one-off familiarisation and gap analysis costs (estimated using our SCM), there is a one-off cost to set up a register using our template and a yearly ongoing cost to update it. These costs are estimated using firms' responses to PRA outreach.

2.26 We do not expect any costs to fall on third parties as firms should already hold enough information to fill out the register with their third party arrangements.

Question 1: **Do you have any comments on the cost benefit analysis including our assumptions, assessment of costs and benefits to firms, consumers, the market and third parties?**

Equality and diversity considerations

2.27 We do not consider that the proposals materially impact any of the groups with protected characteristics under the Equality Act 2010.

2.28 In the meantime, we welcome your feedback on this.

Chapter 3

Reporting operational incidents

3.1 We propose requiring firms to submit reports of operational incidents that breach defined reporting thresholds. The rules will define what we consider to be an incident and set out the thresholds. Firms will need to assess the impact or potential impact of the incident against the thresholds, and report the incident to us if it breaches one or more of them.

3.2 The purpose of these proposed requirements is for us to receive sufficient, consistent, and timely information about incidents to:

- assess, triage and work with firms to manage the potential impact of operational incidents on consumers, firms, or markets
- get a better understanding of the operational resilience of individual firms and the financial services sector more broadly
- identify potential vulnerabilities and areas for improvement

3.3 When firms experience operational incidents, they need to fulfil their obligations to us under Principle 11 and the SUP 15.3 General Notification Requirements by reporting operational incidents in line with the proposals set out in this CP.

Operational incident

3.4 We propose the following definition of an operational incident:

A single event or a series of linked events that disrupts the firm's operations, where it either:

- disrupts the delivery of a service to the firm's clients or a user external to the firm; or
- impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to the firm's clients or a user external to the firm

3.5 Firms should only report operational incidents that breach the proposed thresholds in the way we have set out in this CP. Firms should continue to report other matters as they currently do.

Question 2: **Do you agree with the proposed definition of an operational incident?**

Reporting Thresholds

3.6 We propose that firms must report an incident when they think it breaches one or more of the proposed thresholds. These thresholds are based on an incident's actual or potential impact on our wider organisational objectives. We have taken a proportionate approach to avoid creating any unnecessary burden to firms. The reporting requirements will target only the incidents with a significant impact on our objectives.

3.7 Firms should assess the impact of an operational incident against 3 thresholds that align to our objectives. The firm will be required to report an incident to us if they consider that one or more of those thresholds is or may be breached. The thresholds are:

1. **Consumer Harm:** The incident could cause or has caused intolerable levels of harm to consumers, and they cannot easily recover as a result.
2. **Market Integrity:** The incident could pose or has posed a risk to market stability, market integrity, or confidence in the UK financial system.
3. **Safety and Soundness:** The incident could pose or has posed a risk to the safety and soundness of the firm and/or other market participants.

Factors to consider when applying the reporting thresholds

3.8 Firms should assess the impact of the incident against the thresholds. It will be for firms to judge which incidents breach the thresholds. Firms may use their existing internal processes to determine whether the scale and potential impact of an incident breaches any of the proposed thresholds.

3.9 When determining if a threshold may have been breached, we do not want to set specific metrics for firms to apply and to measure the impact of the disruption on their services. This is because our rules apply to many firms, which makes a single set of metrics unlikely to be suitable for all types of firms.

3.10 We also do not want to introduce an exhaustive list of incident types which could breach the thresholds. The same type of incident might have a significantly different impact at one firm compared to another. This is due to firms differing in business models, services they provide, position in the market in which they operate, size of their client bases and the type of clients they serve.

3.11 When assessing whether it should report an operational incident by comparing it to the thresholds, firms should also consider a range of factors, including but not limited to the following.

- The direct and indirect impact on the firm's clients or the wider sector.
- The direct and indirect impact on the firm's consumers.
- The firm's ability to provide adequate services.
- The firm's or the sector's reputation.
- The firm's ability to meet its legal and regulatory obligations.
- The firm's ability to safeguard the availability, authenticity, integrity or confidentiality of data or information relating or belonging to a client or user.

The direct and indirect impact on the firm's clients or wider sector

3.12 We expect firms to consider if the operational incident has caused or has the potential to cause, harm to their clients. We also expect firms to consider the impact of the incident on other firms and the wider sector, including and not limited to its counterparties and other market participants.

The direct and indirect impact on the firm's consumers

3.13 When firms assess the impact of the incident against the consumer harm threshold, firms should consider what level of harm may have directly or indirectly resulted. To do this we propose to replicate the concept of intolerable harm that already exists in our operational resilience rules that were published in March 2021 and came into force in March 2022 (PS21/3). Firms in scope of those rules are required to identify and define their important business services that will cause intolerable levels of harm if they were disrupted.

3.14 However, the bar we propose for incident reporting is different from the bar set in our operational resilience rules. For incident reporting, firms should report incidents that have the potential to cause intolerable harm, as well as incidents that have actually caused intolerable harm. This represents a lower bar for firms to report an incident to us. This is because we want firms to tell us about incidents that may cause intolerable harm before that harm crystallises, or where the firms are aware of an incident but do not know the extent of harm it could have caused. We recognise that firms will need to use their own judgements based on their clients and services, when assessing if an incident has the potential to cause an intolerable level of harm.

3.15 Similar to our operational resilience rules, we do not define intolerable harm, as what this constitutes will vary from firm to firm and across sectors. In general, intolerable harm is more severe than inconvenience. For example, this could be where the firm is unable to restore a client's financial position post-disruption, or where there have been serious non-financial impacts that cannot be effectively addressed. This also includes situations where firms are unable to provide consumers with essential services they rely on day-to-day, such as preventing them from accessing their accounts, using ATMs or paying bills.

3.16 To identify where intolerable harm may occur, firms should consider factors other than just the services it provides. This could include the following:

- number and types of clients disproportionately affected by the impact such as vulnerable customers
- financial loss to clients
- financial loss to the firm where this could harm the firm's clients
- level of reputational damage where this could harm the firm's clients

3.17 We also expect firms to consider the implications of the incident on its adherence to the Consumer Duty, and on its ability to continue treating its consumers fairly per our Principles for Businesses (Principles 6 and 12).

The firm's ability to provide adequate services

3.18 We expect the firm to consider whether the operational incident could significantly disrupt the delivery of its services. This could include the firm being unable to:

- provide a business service or services for an extended period of time, particularly where an important business service is disrupted
- meet its obligations to its clients and counterparties
- complete or process a significant number of transactions
- avoid disruption causing harm to clients and counterparties

The firm's or the sector's reputation

3.19 We expect the firm to consider whether the operational incident risks damaging its own reputation, or that of the financial sector. If the incident affects the firm's own reputation, it could breach the safety and soundness threshold. However, if it affects the reputation of, or confidence in, the financial sector, it could breach the market integrity threshold. It could also affect the firm's ability to maintain liquidity and function correctly within the market.

3.20 Where relevant, firms should consider whether an incident could result in a loss of confidence in the firm itself or the wider financial sector. This could include incidents that cause the firm's clients or counterparties to question the firm's business model, its ability to manage risks to the firm and its business model, or the overall stability and strength of the financial market.

3.21 For example, firms should consider whether the incident:

- has, or is likely to have, significant coverage in the media such as social media, local and national news
- could lead to the firm receiving multiple complaints from clients or financial counterparts
- risks the firm losing clients or financial counterparts, with a material impact on its business because of the incident

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

3.22 We expect firms to consider whether the operational incident could result in failure to meet their legal and regulatory obligations. This could include legal obligations to clients, other firms, and market participants (for example, service under a contract); and regulatory obligations to us or other regulators (for example, the ability to comply with rules or submit regulatory returns).

The firm's ability to safeguard the availability, authenticity, integrity or confidentiality of information or data relating or belonging to a client or user.

3.23 We expect firms to consider whether the operational incident could compromise their ability to safeguard information or data belonging to a client or user.

3.24 This includes assets:

- 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

3.25 Examples include, but are not limited to:

- unauthorised access to firm data or firm infrastructure (including office premises) where data belonging to an end user may have been accessible
- loss in sensitive data belonging to an end user
- a cyber-attack on the firm
- an internal server error resulting in data loss

Case studies

3.26 To illustrate how we expect firms to apply the thresholds, we have developed some case studies:

Case study 1: incidents that breach the reporting thresholds

Firms A and B are UK-based retail banks undergoing a merger. During the merger, a failure in the integration of IT systems leaves some clients unable to access their accounts online or via an application. There are also delays in processing client transactions overnight.

The unavailability of the online banking and payment services disrupts clients' day-to-day management of their financial affairs. As the incident has the potential to cause intolerable harm, the firm correctly considers that the potential impact caused by this disruption breaches the consumer harm objectives and should be reported.

Case study 2: incidents that do not breach any reporting thresholds

Firm C is an independent financial advisor. It suffers a power outage which means that the sole director and employee are unable to keep their appointments with their clients. The incident has a minor operational impact with no substantive impact on clients or regulatory obligations. The director correctly considers that the incident has caused an inconvenience but does not have the potential to cause intolerable harm. The firm is not required to report the incident to us, given the impact on services for a small number of clients.

Case study 3: incidents with the potential to cause intolerable harm on clients using the firm's services

Firm D is a debt management plan provider and distributes payments to creditors for its clients. The firm has a supplier that undergoes a technology change programme. An issue with the change results in the firm's payments distribution process being disrupted. This has the potential to cause intolerable harm to consumers, as their debt may not be managed, and creditors may enforce or apply interest to the debts owed to them. The firm correctly considers that the incident breaches the consumer harm threshold and should be reported to us.

Case study 4: incidents causing indirect impact on the firm's clients and wider sector

Firm E provides clearing services to **Firm F**, who in turn provides trade execution services for **Firm G**, a consumer investment firm. Firm E suffers an outage at its data centres, which means it cannot receive orders for clearing trades or ensure that orders are reconciled. As Firm F relies on Firm E for clearing, this disruption means Firm F could not execute trades. The disruption at Firm F leads to a failure to serve Firm G, and prevents clients from trading through Firm G. This can cause intolerable consumer harm as consumers may be unable to buy or sell their investments at a desired price, or their investments may suffer from lower performance because of delayed or failed transactions.

As this incident has caused intolerable consumer harm, Firm G correctly considers that the incident breaches consumer harm threshold and should be reported. Firms E and F correctly consider that the incident breaches consumer harm thresholds for both firms, as they have considered the direct impact of the incident on its clients (for Firm E, Firm F is its client; for Firm F, Firm G is its client), and then the indirect impact on the clients using Firm G's services.

Case study 5: incidents impacting the firm's ability to provide adequate services

Firm H is an insurer that suffers a distributed denial of service cyberattack, which results in its website being taken offline. This means consumers cannot log onto their online banking. The firm is able to divert traffic and reinstate access for consumers, but the firm correctly considers it should report the incident as its services are disrupted, breaching the consumer harm and market integrity thresholds.

Case study 6: incidents that do not affect the firm's ability to provide adequate services

Firm I is a mortgage broker that uses a third party supplier to complete payroll for its employees. Due to a technical issue, the supplier is unable to complete payroll on time this month. The incident causes an operational disruption to the management of the firm's internal affairs, but there is no impact on consumers, to the wider market or on its regulatory obligations. The firm correctly considers that this incident does not breach any of the thresholds so is not required to report the incident to us.

Case study 7: incidents causing indirect impact on the firm's clients and wider sector

Firm J is a trading firm that provides a platform for making security trades. It is the main provider of this service to large firms. The firm suffers a cyber-attack which brings its systems down for several days. Following system recovery, clients are hesitant to reconnect. As a result, they manually upload trade details. This incident has the potential to affect market integrity due to the increased risk of error from clients manually recording trades. This incident also has the potential to affect market stability due to the concentration risk and strain on competitor platforms taking on significantly increased trade loads from clients not reconnecting to the firm. The firm correctly considers that the incident breaches the market integrity threshold and should be reported to us. Under our proposals, we also expect the firm's clients to conduct their own assessment of the impact of the incident against the thresholds, and separately report the incident to us if necessary.

Case study 8: incidents harming the firm's reputation

Firm K is a UK online-only challenger bank that relies on a third party cloud service provider to host its banking system and services. The provider experiences a widespread outage, during which its infrastructure suffers a total outage for several hours, disrupting access for consumers to the firm's online banking services, mobile apps, and consumer transactions across the UK. This has the potential to cause intolerable harm to consumers through major disruption to core banking services, inability for consumers to access their accounts, make payments, or complete transactions. There is also reputational damage due to public scrutiny of the firm's reliance on the cloud provider. Due to the scale of the disruption, the firm correctly considers that the incident breaches the consumer harm and market integrity thresholds.

Case study 9: incidents affecting the firm's ability to meet its regulatory obligations

Firm L is a broker firm that generates orders to match buy and sell sides, by meeting client subscription and redemption requests. The firm uses an order management system (OMS) to help track trade information such as prices and quantities. The OMS is critical to the production of orders and to adjust the firm's portfolio. The OMS suffers a full outage for a few hours, affecting both the firm's clients and the markets in which the firm operates.

This has the potential to cause intolerable harm to consumers as investors may be unable to buy or redeem units in funds, or trade at that time to take advantage of perceived market circumstances.

The outage also has the potential to affect market integrity because the firm's market abuse controls are embedded in the system. As a result, the market abuse controls were not operating during the outage. As such, some trades may have been processed during the outage without going through market abuse controls. The firm correctly considers that the incident breaches both the market integrity and consumer harm thresholds and should be reported to us.

Case study 10: incidents affecting the firm's ability to safeguard the confidentiality of assets relating to its clients

Firm M is a credit broker and suffers a cyber and ransomware attack resulting in consumer data being exposed on the dark web. The firm correctly considers that the incident breaches the consumer harm threshold and should be reported to us, as well as to the Information Commissioner's Office (ICO).

Question 3: **Do you agree with the thresholds for firms to apply when considering reporting an operational incident to us? Are there other factors firms should consider when reporting operational incidents?**

Approach to reporting operational incidents

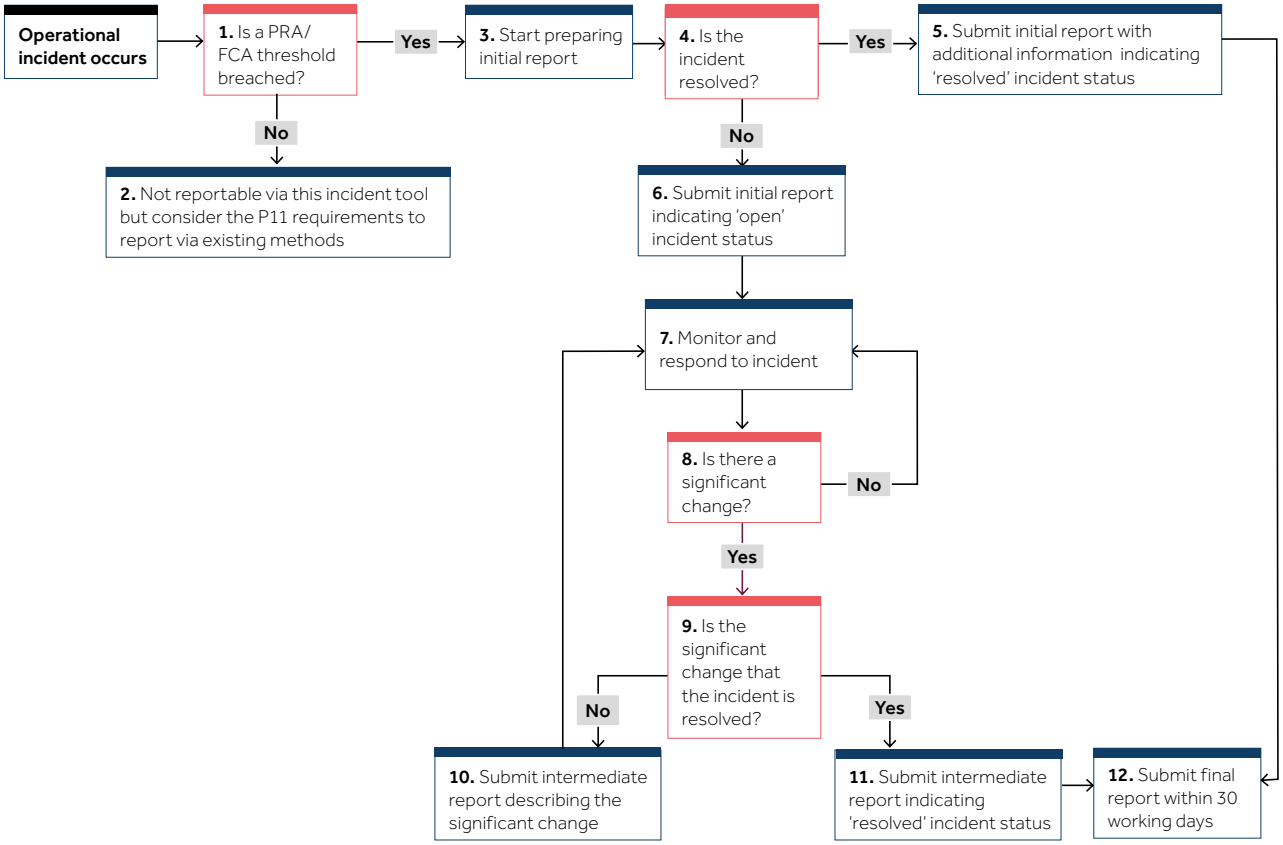
3.27 When firms consider that an operational incident breaches a threshold, we propose that firms provide the below (see Figure 1).

- An Initial Incident Report, including where the incident is resolved shortly after it occurs.
- One or more subsequent Intermediate Incident Reports updating on the progress of the incident, including when it is resolved.
- A Final Incident Report.

Process for reporting incidents: When to report

3.28 The following diagram sets out how firms should report the management of an operational incident to us. To help, we intend to give firms templates to complete at each stage of reporting for firms to provide certain information and data to us. This will enable us to understand the impact of the incident.

Figure 1: Proposed incident reporting process



3.29 The firm must report an incident that has breached one or more of the thresholds as soon as it is practical to do so.

3.30 After the firm submits the initial report, if we consider that the incident poses a risk to our statutory objectives, we may contact the firm for more information or supervise the firm's response to the incident.

3.31 The firm should update us on the management of the incident after any significant change, and as soon as it is practical to do so. The firm can do this by submitting an intermediate report. The firm may need to submit more than one intermediate report if there are multiple significant changes.

3.32 However, we recognise that the firm's understanding of an incident may not be fully formed, especially at the outset of an incident, when details of the incident, impact and potential cause are still being established.

3.33 We will not expect the firm to divert resources to report the incident at the expense of taking actions to resolve the incident or take urgent steps necessary to mitigate the impact of the incident.

3.34 We do however expect the firm to provide timely, ongoing updates on the progress of an incident, with the provided information being as accurate as possible, as the firm's understanding of the incident develops.

3.35 After the incident is resolved, the firm will submit a final incident report within 30 working days. The report should confirm the details of the incident, the impact of the incident, the root cause of the incident, any lessons learned and any additional steps the firm is taking. Where this is not practicable, the firm should submit the report as soon as is practicable, but not more than 60 working days from when the incident was resolved.

Format of incident update reports: What and how to report

3.36 Following engagement with industry as part of the Transformation Data Collection, we propose that firms submit incident reports via an online platform to be developed.

3.37 We propose to provide a template for firms to complete at each stage of the incident reporting process. To help reduce the burden on firms, the reporting solution will use auto-population and conditional field logic based on information we already hold. This will make the reporting process as straightforward and efficient as possible.

3.38 Using the templates will help us to triage, assess and work with firms to manage the impact of the incident more efficiently. Firms can also add additional information in free form text boxes, as well as add attachments.

Initial incident report

3.39 We recognise the importance of balancing our need to receive timely incident information with firms' need to devote resources to resolve an operational incident. So, we ask that firms submit the initial incident report *as soon as is practicable* once a crystallised operational incident has breached a threshold.

3.40 We want to reduce the firm's burden while it focuses on resolving an incident. So, we propose that firms submit only the minimum information we require to assess potential risk to our objectives. This will help us understand the nature of the incident, the service(s) impacted and what actions the firm may be taking, or has taken, to resolve the incident.

3.41 In some circumstances, we may reach out to the firm directly to understand the details, impact of the incident and the steps they are taking. This engagement will not change the reporting obligations proposed in this CP.

3.42 If the firm has resolved an incident before submitting an initial report, we propose that the firm lets us know that the incident has been resolved as soon as is practicable within the initial report. The firm then has 30 working days to follow up with the final incident report with the root cause. The firm will not need to submit an intermediate incident report in this scenario.

Intermediate report

3.43 The main purpose of the intermediate report is to give us timely progress updates. This includes any actions that the firm is taking towards resolution or new information that may have come to light since the initial report.

3.44 We propose that firms submit an intermediate report as soon as is practicable after any significant change in circumstances. Examples of when to submit an intermediate report include the following.

- When additional information is available that provides more context on the incident.
- When the known impact of an operational incident changes.
- When the firm identifies the origin or root causes of the incident.
- Where information previously submitted to us in error needs to be corrected or materially clarified.
- When the firm has taken action to mitigate the impact of the incident.
- Whether any mitigation action has been successful or not.
- Whether the firm has deployed a business continuity plan.
- When the incident is resolved.

3.45 When the operational incident is resolved, firms will be required to submit an intermediate report confirming this. The firm will complete the incident closure section confirming what the firm believes to be the cause of the incident at that time, the understood impact of the incident and remedial actions the firm has taken. This will help us to understand possible risks and vulnerabilities to the firm, its clients and the wider financial sector, and gain assurances that firms are taking the appropriate measures to fix identified vulnerabilities. The full impact assessment of the incident on the firm, its external clients, and the financial sector will not be required in this report. This will be provided in the final incident report.

Final incident report

3.46 After confirming the resolution of an operational incident, we expect firms to submit a final report within 30 working days. The final report should confirm the details of the incident, provide a full impact assessment, the root cause of the incident and any lessons learned, or additional measures taken. Firms will also be able to submit their own reports or documents in various formats during this stage via our platform.

3.47 If an operational incident originates at a third party, we propose that the firm takes reasonable steps to get information about the root cause of the incident from the third party.

Question 4: **Do you agree with the proposed approach to standardise the formats of incident reporting?**

Operational incident data

3.48 For each of the incident reports, firms are required to provide information on the ongoing status of the operational incident. To facilitate this, we ask firms to submit this information under 4 categories: reporting details, incident details, impact assessment and incident closure (see Table 1). The details of all the fields we are requesting in the templates are in **Appendix 2**.

Table 1: Data categories for 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, description, service(s) disrupted, time of incident and actions the firm intends to take/has taken to recover.
Impact Assessment	Details of the impact of the operational incident, including number of consumers/clients affected, reputational impact, volume and value of transactions affected and parties affected.
Incident Closure	Details of the root cause(s), lessons learned and possible remedial actions.

3.49 We propose to vary data fields depending on the nature of the operational incident. For example, third party details will be required for a third party incident.

Question 5: **Do you agree that we are being proportionate and is collecting the right information at the right time to meet its objectives? Is there other information that should also be collected for a better understanding of the operational incident?**

Alignment with international standards

3.50 The increased interconnectedness and complexity of the financial system makes it more likely that an operational incident at one firm or service provider could escalate across sectors and borders. Firms operate in multiple jurisdictions and increasingly rely on services provided by global third party service providers. So, the potential systemic risks arising from a failure, or severe disruption to their services could spread beyond the UK. Internationally active firms and FMIs have also noted that fragmented regulatory and supervisory practices can be detrimental to their operational resilience and increase compliance costs.

3.51 Consistent international standards for reporting incidents are crucial for effective incident response. Recognising this, the FSB published a report on achieving greater convergence in cyber incident reporting in April 2023. It is also developing a common incident reporting standard, Format for Incident Reporting Exchange (FIRE). Financial regulatory authorities can adopt and use this format to collect information on operational incidents from firms.

3.52 Where possible, our proposed rules are aligned with other incident reporting regimes and international standards, such as the FSB's FIRE and the EU's DORA regime. This alignment will allow us to exchange information on incidents with other regulators

more effectively and consistently under existing legal gateways. We also believe it will increase reporting efficiency for international firms subject to multiple incident reporting requirements.

3.53 The requirements in this CP do not replace firms' obligations to make notifications under the Payment Services Regulations 2017, which implemented the Payment Services Directive (PSD2). However, we do not expect all PSD2 notifications will meet the thresholds for reporting incidents under our proposals. So, there may be instances where firms will be required to report an incident under our current proposals in addition to a PSD2 notification.

Chapter 4

Reporting third party arrangements

4.1 In this chapter we explain our proposals for a sub-set of firms (as set out in 1.7) to:

- expand the scope of existing outsourcing notifications, covering both material outsourcing and material non-outsourcing arrangements (collectively referred to as 'material third party arrangements') for in-scope firms
- provide a template for firms to submit notifications of changes to these arrangements or new ones
- require firms to maintain and submit a register of these arrangements to us, ensuring this is up to date annually

4.2 Under current requirements, we receive limited and inconsistent data on third party arrangements relating only to firms' outsourcing arrangements. This has resulted in gaps in our knowledge of potential risks that third parties pose to individual firms and the financial services sector. We are proposing to introduce material third party reporting rules, which includes outsourcing and non-outsourcing arrangements, for a sub-set of firms (as set out in 1.7) that have the biggest consumer and market impact.

4.3 Over the years, firms' operations have become more complex and dependent on technology, increasingly relying on a wide range of services delivered by third parties. To support operational resilience, firms need to effectively manage risks posed by all their third party arrangements which are material, not just a sub-type of third party arrangements that are classed as outsourcing (see examples in 4.4 below). It is important that firms manage their third party risk appropriately, as disruption to third parties could harm the firm, its consumers, or threaten the stability of the financial system.

4.4 Below are scenario-based examples illustrating where a defect or failure in the performance of a third party arrangement directly impacts the firm.

- Firm 1 uses a third party to automate fraud monitoring. A system failure at the third party prevents the tool from functioning, leaving the firm and its consumers vulnerable to fraud. A lack of fraud detection results in Firm 1's consumers being subject to increased risk of fraud.
- Firm 2 relies on a third party cloud data centre to process data for its operations. The data centre experiences a failure during a system update, leaving the firm unable to access data which impacts the delivery of multiple important business services. The disruption adversely impacts a large proportion of its consumer base for an extended period.
- Multiple firms rely on a third party provider to perform their payment settlement services. The third party experiences a major operational disruption which leads to delays in the settlement of payments over a few hours. This incident prevents payment transactions from being settled, leading to consumer harm and market disruption.

4.5 Our rules currently address material outsourcing arrangements explicitly, but do not mention non-outsourcing arrangements which may limit our visibility over the relevant risks. Examples of third party arrangements that are not classified as outsourcing could include the purchase of data, hardware, software, and other ICT products, such as the design and build of an on-premise IT platform. Similar to outsourcing, a firms' ability to deliver important business services will be impacted if these third party services were disrupted.

4.6 Additionally, our existing requirements for firms to notify us of any new outsourcing arrangements or changes to them, are not structured. This makes the data more difficult to use and limits the interaction between our existing notifications requirements and our proposed third party register data.

4.7 To address this, we propose to expand the scope of our data collections from material outsourcing arrangements to include material non-outsourcing arrangements, collectively referred to as 'material third party arrangements.' The change will result in the introduction of the proposed definitions for 'third party arrangement' and 'material third party arrangement' in our Handbook. We also intend to provide a template for firms to submit this information in a structured format to us. This will promote greater transparency in supply chains, allowing us to identify firm-specific and systemic risks, minimise consumer harm and market disruption.

4.8 The proposals in this chapter will result in changes to:

- notification requirements in SUP 15.3 (General Notification Requirements) and the new section SUP 15.19 (Notification of material third party arrangements)
- reporting requirements in the new section SUP 16.33 (Material third party arrangements register)

Material third parties

4.9 We propose to define a 'third party arrangement' as:

An arrangement of any form between a firm and a service provider. Whether or not the product or service is:

- one which would otherwise be provided by the firm itself
- provided directly or by a sub-contractor
- provided by a person within the same group as the firm

4.10 This is in line with the definition in the Third Party Elements and EBA Guidelines on ICT and security risk management. This encompasses outsourcing and non-outsourcing third party arrangements.

4.11 When identifying third party arrangements, firms should consider their use of those products and services. For example, we will expect to see:

- products provided by third parties directly used for the firm's operations (eg software)

- services provided by third parties either to directly support the firm's operations (eg the third party's technical support hours), or to support the firm's use of a product in support of the operations (eg the service to provide content updates to the software)

4.12 With the above considerations, and to make sure we collect relevant information at a proportionate cost to firms, we propose to only collect information on firms' 'material third party arrangements'. These are highly important third party arrangements, where a disruption or failure in performance of the product or service provided, could do any one or more of the following:

- cause intolerable levels of harm to the firm's clients
- pose a risk to the soundness, stability, resilience, confidence or integrity of the UK financial system
- cast serious doubt on the firm's ability to satisfy the threshold conditions, or meet its obligations under the FCA's Principles for Business, or under SYSC 15A (operational resilience)

4.13 If a firm deems a third party arrangement as 'material', it should implement controls that are appropriate to the materiality of the arrangement. These controls do not have to be the same as those that apply to outsourcing arrangements (as specified within SYSC 8) and should be adapted or changed as necessary. The scope and nature of controls should reflect the significance of the materiality of the third party arrangement.

4.14 When determining materiality of a third party arrangement, firms need to consider their impact. Factors to be considered include but are not limited to the following:

- direct connection to the performance of a regulated activity
- size and complexity of the business area(s) or function(s) supported by the third party arrangement
- the potential impact of a disruption, failure or inadequate performance of the third party arrangement on the firm's:
  - business continuity, operational resilience, and operational risk, including
    - conduct risk
    - ICT risk, ie the risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change information technology (IT) within a reasonable time and with reasonable costs when the environment or business requirements change (ie, agility)
    - legal risk
    - reputational risk
  - ability to
    - comply with legal and regulatory requirements
    - conduct appropriate audits of the relevant function, service or service provider
    - identify, monitor and manage all risks
  - obligations under
    - the FCA Handbook

  - the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity of the institution or payment institution and its clients, including but not limited to the UK General Data Protection Regulation and the Data Protection Act 2018
  - counterparties, consumers or policyholders.

- the firm's ability to scale up the third party service.
- the firm's ability to substitute the service provider or bring the outsourced service back in-house, including estimated costs, operational impact, risks, and timeframe of doing so in stressed and non-stressed scenarios.

4.15 We do not intend to change the definition of 'material outsourcing'. We propose in-scope firms (as set out in 1.7) should notify us of entering or significantly changing a material outsourcing arrangement, in line with the proposed requirements for material third party arrangement notification. This will mean they do not need to notify us twice. However, all other firms should continue complying with their existing obligations under SUP 15.3.8. Firms need to notify us before entering or significantly changing a material outsourcing arrangement, and under SYSC 8 and SYSC 13.9.

4.16 To reduce the burden on firms, we propose the following third party products or services, are out of scope for the purposes of submitting information.

- Functions that are statutorily required to be performed by a service provider a related information which is already received by the regulators (for example, statutory audit, CASS audit).
- Basic utilities, for example, electricity, water, gas (excludes telecommunication and internet service providers).

Question 6: **Do you agree with the proposed definition of third party arrangements?**

Question 7: **Do you agree with the proposed definition of material third party arrangements?**

Notifications

4.17 We currently only require firms to notify us of material outsourcing arrangements in line with SUP 15. The rules do not specify a particular format, resulting in unstructured reporting. This makes it more difficult to analyse, identify, and understand any potential or emerging risks, as well as compare the data across firms.

4.18 We want assurance that firms have properly considered the risks posed by the arrangements that are most fundamental to their operational resilience. Regulators will be particularly interested in whether firms have integrated the arrangement to meet the requirements of our operational resilience requirement and the expectations set in SYSC 8.

4.19 We propose the following changes within our Handbook.

- Include new rules and guidance in SUP 15.19 (notification of material third party arrangement) to capture notifications of firms' material third party arrangements to reflect our proposals in 4.1.
- Include new rules and guidance in SUP 15.3 that in-scope firms should notify us of entering or significantly changing a material outsourcing arrangement under the new section SUP 15.19. This will mean that they do not need to notify us twice. This does not change the obligation for all other firms to notify us of entering or significantly changing a material outsourcing arrangement under SUP 15.3.8(1)(e).

4.20 We propose to expand the scope of the data collection to capture material outsourcing and non-outsourcing third party arrangements. But we do not propose to change the timeframes for firms to submit related notifications. Firms should continue to submit a notification ahead of entering or significantly changing a material third party arrangement. We will continue to use these notifications to conduct appropriate regulatory scrutiny and have adequate oversight over risks to our objectives.

4.21 We have considered how to standardise the way firms submit material third party notifications by specifying a template. We propose this will provide clear expectations on the minimum information required and simplify the reporting process for firms.

Question 8: **Do you have any comments on our proposed notification requirements including the impact on the number of arrangements that will be reported?**

Register

4.22 We propose that firms maintain and submit a structured register of their material third party arrangements. As part of our current notification arrangements (SUP 15.3.8), firms should already have records of material outsourcing arrangements. We also consider that firms will record and make available any additional relevant information of which we reasonably expect notice, in line with Principle 11.

4.23 We require firms to submit their registers annually using an FCA platform. The firm's register should include information such as:

- data on the regulated firm
- data on third parties including intra-group arrangements
- data on types of services being performed by a third party
- data on products and services used
- information on supply chain
- information on firms' assessments of their third party arrangements (see Table 2)

4.24 Collecting data on firms' third party dependencies in a structured format through a central register enables us to take a more data-led approach for both firm-specific and broader considerations. In particular, to:

- assess firms' compliance with both the proposals on material third party arrangements, and the existing requirements on outsourcing, including SUP15 (for notifications), SYSC 8 and SYSC 13.9 of the FCA Handbook (on outsourcing requirements for applicable sectors)
- gain a better understanding of the risks in firms' material third party relationships and potential changes to the operations of the firm
- collect supervisory insights on an individual firm's levels of third party usage.
- help the regulators better understand the impact of an incident, caused by a third party, on the broader financial sector
- monitor the financial sector's reliance on third parties to support the identification of potential CTPs, which we will recommend to HM Treasury to consider for designation under the CTP regulatory regime

Information to submit to us

4.25 To minimise the reporting burden, our proposed templates for notifications and the register are as aligned as possible. We have also developed these templates, having considered: the existing ones used for our voluntary Outsourcing Register data collection and our lessons learned from this exercise; and where appropriate aligned with the EBA Outsourcing Guidelines, and the EU Digital Operational Resilience Act (DORA) ICT Services Register.

4.26 Table 2 summarises the data we set out to collect. The full proposed template and guidance for completion are in **Appendix 3**.

Table 2: Proposed data field categories to be collected

Data bucket	Description
Primary data on regulated firms	Details on the firm submitting material third party arrangement information. This includes firm identification and submission references.
Primary data on third parties, including intra-group arrangements	Details of the third party service provider firms have an arrangement with, including the name, registered address, and legal identifiers of the service provider.
Data on types of services being performed by a third party	Information on the services being provided by an external third party service provider. This includes a description of the service, whether the service supports an important business service, and where the service is being performed.
Data on products and services used	Information on the type of service being provided by an external third party.

Data bucket	Description
Information on supply chain	Ranking of third party providers for each service included in the scope of each contractual arrangement.
Data on assessments	Information on firms' due diligence conducted for each arrangement. This includes details on risk assessments, recent audits, and review from the appropriate Senior Management Functions.

4.27 The proposed template comprises six data groups (shown in the table above). These are underpinned by specific taxonomies and are linked to each other using data fields to form a relational structure that enables us to form a view of the third party supply chain. These include the firm identifier, contractual arrangement reference numbers, third party provider name and legal entity identifiers (LEIs), and the supply chain rankings.

4.28 We want to be able to assess the extent of concentration of third party providers supporting specific business services. So, firms will be required to submit data on the types of services being performed by a third party, including whether this is an important business service for the firm.

4.29 To reduce the regulatory burden on firms and to enable consistent data analysis of the types of third party products and services firms use, we propose firms choose from a set list of what type of third party services they use. The proposed list aligns with the EU's DORA Final Report on draft ITS on Register of Information Annex III Type of ICT services taxonomy, but is modified to include additional relevant non-ICT services.

4.30 To support our understanding of firms' third party supply chain, firms will 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 in the supply chain. The first external service provider that the firm is purchasing from directly will always have a 'rank' number of '1', with lower numbers denoting the closeness of the arrangement to the firm (eg providers with rank '2' would be an external provider's supplier).

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

4.32 To be proportionate, we propose to only require firms to identify service providers within the supply chain whose disruption will impair the continuity of the firm's service, irrespective of the rank. This is broadly aligned with the approach in Article 28 of the EU's DORA. This will allow us to link all material third party product or service providers who are part of the same supply chain and indicate where n^{th} party concentration risks may arise.

4.33 We also propose to require firms to submit some basic information on their assessments of material third party arrangements. This will enable us to assess firms' compliance with the SYSC 8 requirements and expectations set out in FCA Handbook.

Question 9: Do you think the mechanism to submit and update the structured register of firms' material third party arrangements is proportionate?

Question 10: Do you have any comment on the template which includes the information on third party arrangements to be shared with us?

Annex 1

Questions in this paper

Question 1: Do you have any comments on the cost benefit analysis including our assumptions, assessment of costs and benefits to firms, consumers, the market and third parties?

Question 2: Do you agree with the proposed definition of an operational incident?

Question 3: Do you agree with the thresholds for firms to apply when considering reporting an operational incident to us? Are there other factors firms should consider when reporting operational incidents?

Question 4: Do you agree with the proposed approach to standardise the formats of incident reporting?

Question 5: Do you agree that we are being proportionate and is collecting the right information at the right time to meet its objectives? Is there other information that should also be collected for a better understanding of the operational incident?

Question 6: Do you agree with the proposed definition of third party arrangements?

Question 7: Do you agree with the proposed definition of material third party arrangements?

Question 8: Do you have any comments on our proposed notification requirements including the impact on the number of arrangements that will be reported?

Question 9: Do you think the mechanism to submit and update the structured register of firms' material third party arrangements is proportionate?

Question 10: Do you have any comment on the template which includes the information on third party arrangements to be shared with us?

Annex 2

Cost benefit analysis

Introduction

1. The Financial Services and Markets Act (2000) requires us to publish a cost benefit analysis (CBA) of our proposed rules. Specifically, section 138I requires us to publish a CBA of proposed rules, defined as 'an analysis of the costs, together with an analysis of the benefits that will arise if the proposed rules are made'.

2. This analysis presents estimates of the significant impacts of our proposal. We provide monetary values for the impacts where we believe it is reasonably practicable to do so. For others, we provide a qualitative explanation of their impacts. Our proposals are based on weighing up all the impacts we expect and reaching a judgement about the appropriate level of regulatory intervention.

3. The CBA has the following structure:

Incident Reporting (IR)

- Operational incidents in the financial sector
- Problem and rationale for intervention
- Options assessment
- Our proposed intervention

Third Party Reporting (TP)

- The Market
- Problem and rationale for intervention
- Options assessment
- Our proposed intervention

Appraisal

- Baseline and key assumptions
- Summary of impacts
- Benefits
- Costs
- Wider economic impacts
- Monitoring and Evaluation

4. The CBA separates the proposals (IR and TP) for the purposes of establishing the market, harm, baseline, intervention, and options. Costs and benefits are assessed for both proposals together, split by theme. For dual-regulated firms, these costs are aligned with those presented in the PRA's CBA and not additional to those published by the PRA. Rather, this CBA solely reflects the costs of our proposals.

Incident Reporting

Operational incidents in the financial sector

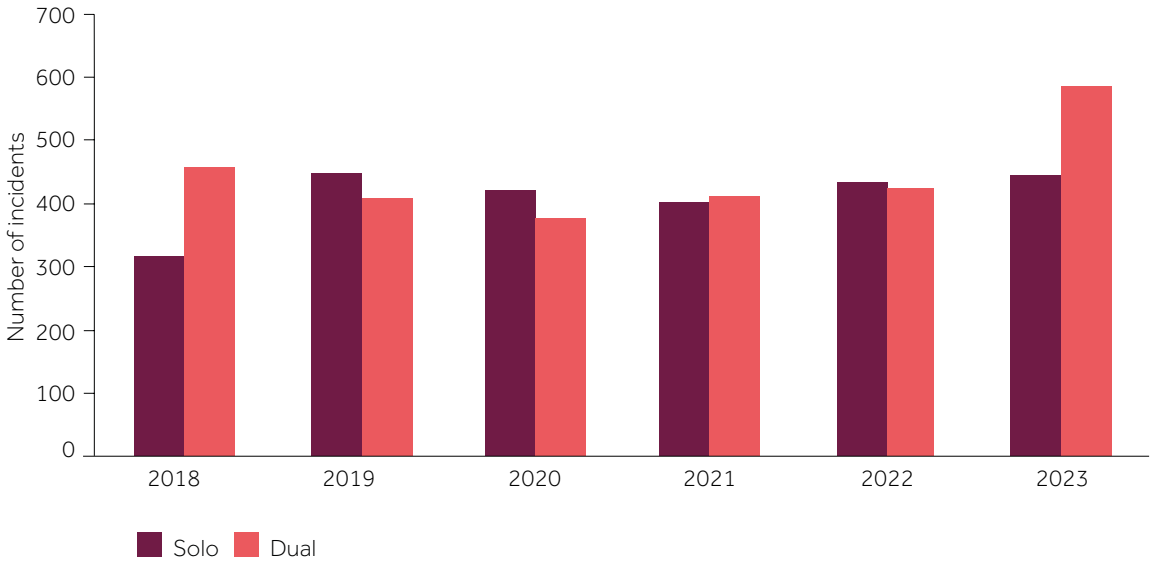
5. Operational incidents in the financial sector which materially disrupt a firm's services may have a wider indirect impact on the market. Particularly when inter-firm services and dependencies, such as cloud service providers, are considered, a large-scale material disruption could affect cross-market stability and cause losses for consumers or firms.

6. All directly regulated firms are required to report operational and material incidents to the FCA (c. 41,500 firms) and, if dual-regulated, the PRA (c. 1,500 firms). The rules and guidance are set out under the Supervision (SUP) module of the FCA Handbook. The existing requirements are contained within PRIN 2.1 The Principles – FCA Handbook. Principle 11 states:

'A firm must deal with its regulators in an open and cooperative way, and must disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice.'

7. Since 2018, firms have reported 5,351 incidents to us. The number of notifications per year remained stable until a 20% rise in 2023 driven by an increase in incidents reported by dual-regulated firms. The types of incidents reported include cyber-attacks, third party failures, change management issues, hardware and software issues amongst others.

Figure 1: The number of incidents reported to the FCA (2018 – 2023), by solo- and dual-regulated firms



Source: FCA internal incident management data

Problem and rationale for intervention

Harms

8. Incidents can cause harm affecting not only consumers, firms, other market participants in the financial services (FS) sector, but also the wider economy. Incidents can cause large-scale disruption.

9. For example, harm to consumers may arise from disruption to banking services, which may affect the ability to make payments, access accounts or receive insurance claims payments. These types of disruption undermine confidence in the financial system and can cause substantial emotional distress.

10. Harm to market participants and to the wider economy may arise from disruption to financial markets' operations, such as the forced closure of trading venues following a cyber-attack and the potential threat to market and supplier confidence that can result from a substantial disruption.

11. Harm to market participants and market integrity may arise from, for example, the failure of a shared facility or market infrastructure on which the functioning of a market depends, uncontrolled access to, and misuse of, market sensitive data, or the inability to access market pricing data.

12. The harm caused by operational incidents can be high, not only in terms of financial losses but also in non-financial terms, such as reputational harm to firms and markets and causing distress in the day-to-day lives of consumers. The range and complexity of impacts, such as non-financial impacts make it difficult to fully estimate on the total cost of the disruption caused. However, some recent high-profile incidents have resulted in either regulatory fines or firms publicly stating associated losses (all figures are adjusted to 2024 prices from source).

- In 2018, a failed migration to a new IT system cost TSB £412.16 million, including consumer redress, rectification, and associated remediation resource costs of £156.28 million. The FCA and PRA jointly fined TSB £52.86m in 2022 after conducting an investigation into the failures that occurred.
- In 2014, the FCA and PRA fined RBS, NatWest and Ulster Bank a total of £74.66m. This was because an IT failure in 2012 led to widespread disruption, affecting consumers' ability to access accounts and make payments and the banks' ability to participate in clearing which affected the financial markets. We noted that RBS had paid remediation of £93.73m to affected consumers at the time of its report.

13. In our CBA in CP19/32 – Building operational resilience we found that 87 firms out of a sample of 306 respondents identified at least 1 incident in the last 5 years up to 2019 that led to quantifiable costs to their business, totalling £115.10m. Some of these firms identified just the total cost of a range of incidents, others separately identified individual incidents. A total of 108 individual incidents were reported to us, accounting for £83.16 million of the total costs of £115.10m identified and with an average cost per incident of approximately £0.77m.

14. Negative externalities arise when firms' approaches to the prioritisation of operational risks may not reflect the impact of operational disruptions on third-parties reliant on firms' services. Consequently, operational risk management may not be commensurate with the potential harm to consumers and markets that could arise from an incident. This leads to underinvestment in operational resilience, in turn leading to negative externalities when the cost of incidents falls disproportionately on the consumers and not the firms.

15. Harm caused by incidents may be more severe if they are not reported to the FCA and the PRA ('the regulators') in a timely manner, with all the information required to intervene and manage an incident. This is because the time the regulators takes to react to and manage the incident, as well as to limit and address harms arising from it, will be longer.

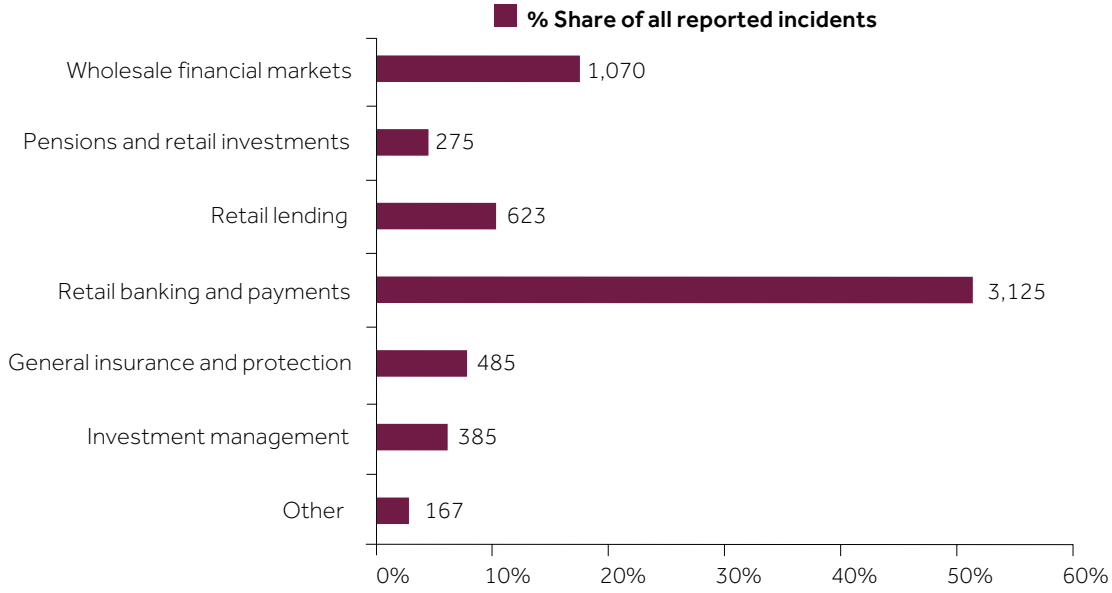
16. Our operational resilience policy (PS21/3) seeks to address this market failure. However, we acknowledge that, inevitably, incidents will continue to occur and require management to minimise harm.

Drivers of harm

17. We do not currently receive incident reports in a consistent and timely manner, delaying our intervention and management of incidents, which may be caused by multiple factors.

18. Firstly, there may be an information asymmetry where firms may not be reporting all incidents to us. Of our directly regulated firms (c. 41,500) only around 1,000 reported an incident between 2018 and 2023. Incident reporting is also inconsistent amongst our defined firm sectors, with firms in the wholesale financial markets sector and retail banking and payments sector reporting 70% of incidents. While these concentration patterns suggest that there may be some underreporting, we cannot quantify the scale of it. Underreporting carries a large risk as this makes it more difficult for us to help minimise consumer harm from an incident and identify market-wide operational risks.

Figure 2: Proportion and volume of incidents reported by firms to the FCA in each sector (2018 – 2023)



Source: FCA internal incident management data

19. Since 2018, over 20% of operational incident reports submitted by firms arrived over 11 days after the incident had started. Reporting several days so long after the incident carries a higher risk that the incident will escalate before we can assess it and manage the impact under our objectives to protect consumers and market integrity. A European Securities and Markets Authority report on cloud outsourcing and financial stability risks concludes that 'in financial settings where longer outages cause systemic costs... Cloud Service Providers can best address systemic risks by strongly reducing incident resolution times, rather than incident frequency'.

20. Secondly, there is a regulatory failure as the regulations that govern incident reporting are not sufficiently detailed. There is currently no standardised template with guidance for firms to use when reporting incidents. This can create an inefficient process of follow-up conversation with firms, as we seek to gather necessary information to both address the specific incident and identify trends and emerging risks.

21. As the data is not standardised when we receive it, it must be manually processed. This is time-consuming and introduces the possibility of human error, and results in the incident management team taking longer to triage, respond to, and escalate incidents. This time could have otherwise been spent managing the incident and any fallout arising from it, possibly reducing the harm caused.

22. Our guidance provided to firms concerning incident reporting is not as detailed as it could be, nor is it aligned with the PRA's. This is an unnecessary burden on firms who must interpret requirements under both sets of rules, and this increases the time spent following up with firms to gather the required information.

Options

23. We assessed several options before choosing the proposed intervention. These covered different incident reporting thresholds and criteria by which incidents may be categorised. The options are presented summarised in Table 1.

Table 1: Options assessment for incident reporting

Option	Assessment
No change in reporting rules; improve guidance for firms on when and how to report incidents.	This option does not cause much disruption to firms, who are already familiar with existing processes. However, this option is not preferred as it may not target the root cause of incident reporting issues, such as reporting several days after the incident has occurred or underreporting.

Option	Assessment
Staggered thresholds for reporting: **1.** Firms in scope of operational resilience policy (PS21/3) report incidents which cause harm, defined as a negative outcome to consumers and markets because of an operational incident disrupting one or more important business services. **2.** All firms report incidents which cause intolerable harm, defined as an outcome which consumers cannot easily recover from, for instance where, post disruption, a firm is unable to put a client back into a correct financial position, or where there have been serious non-financial impacts that cannot be effectively remedied. **3.** All firms report data breaches, cyber incidents, or incidents which lead to reputational risk or material revenue loss.	This option will be a large change to the incident reporting process and rules. It may help us focus on incidents based on relative priority, ensuring that reporting is proportionate. It also aligns with the PRA's rules for firms in scope of operational resilience policy. However, this option is not preferred as it may result in a high volume of low impact incident reports, and by focussing on important business services in our rules, incidents not related to these may not get reported.
Firms report low, medium, and high impact incidents based on different categories of financial, operational, and reputational impact as well as FCA objectives.	This option provides some clarity on our expectations and incident types. Firms will decide when to report incidents based on the impact criteria. However, this option is not preferred as there is a risk that the regulatory burden will be disproportionate. Firms need to adjust to thresholds and categories that may not align with their internal metrics.
Align reporting criteria to FCA objectives and add a non-exhaustive list of examples to provide further clarity on which incidents we want to be notified of.	This option clearly articulates the impact and materiality thresholds for incidents. It focuses on incidents that could result in harm, ensuring that reporting is proportionate. For example, firms will be supported through guidance and examples that clarify our expectations. This is the preferred option we are consulting on.

Our proposed intervention

24. We propose to set out rules-based regulatory reporting requirements to standardise the routine reporting of operational incidents. The proposed rules specify which types of incidents firms should report to us, when to report, and introduce a standardised template for doing so. We intend our proposals to be compatible, where possible, with broader international standards and requirements, which may help firms that must report incidents in multiple jurisdictions. The intervention supports our strategic commitment to minimise the impact of operational disruptions by refreshing rules around how and when firms report incidents to us.

25. We are developing a single system which will automate the end-to-end submission of data. This will help ensure we can assess and respond to operational incidents in a more timely, proportionate, and informed manner.

26. This rule will apply to all directly regulated firms; however, there are some mitigations in place to ensure that the burden on small firms is proportionate.

27. There are existing rules on incident reporting that apply to all firms; therefore, the burden to report incidents already is already present. We believe that providing a structured format for reporting those incidents will not increase the burden on firms above current requirements. We are not proposing to collect new information.

28. We expect structured reporting of incidents with clear guidance on when and which incidents to report will reduce the burden on smaller firms where they do not have existing incident management processes. We also anticipate a lower burden on smaller firms when reporting incidents as they will spend less time and resource responding to regulators' information requests.

29. We have calibrated the thresholds in a way that means the probability of smaller firms reporting incidents is lower, therefore we expect smaller firms will report fewer incidents.

30. Table 2 below sets out the difference between the current and proposed rules.

Table 2: How our new requirements differ from existing requirements

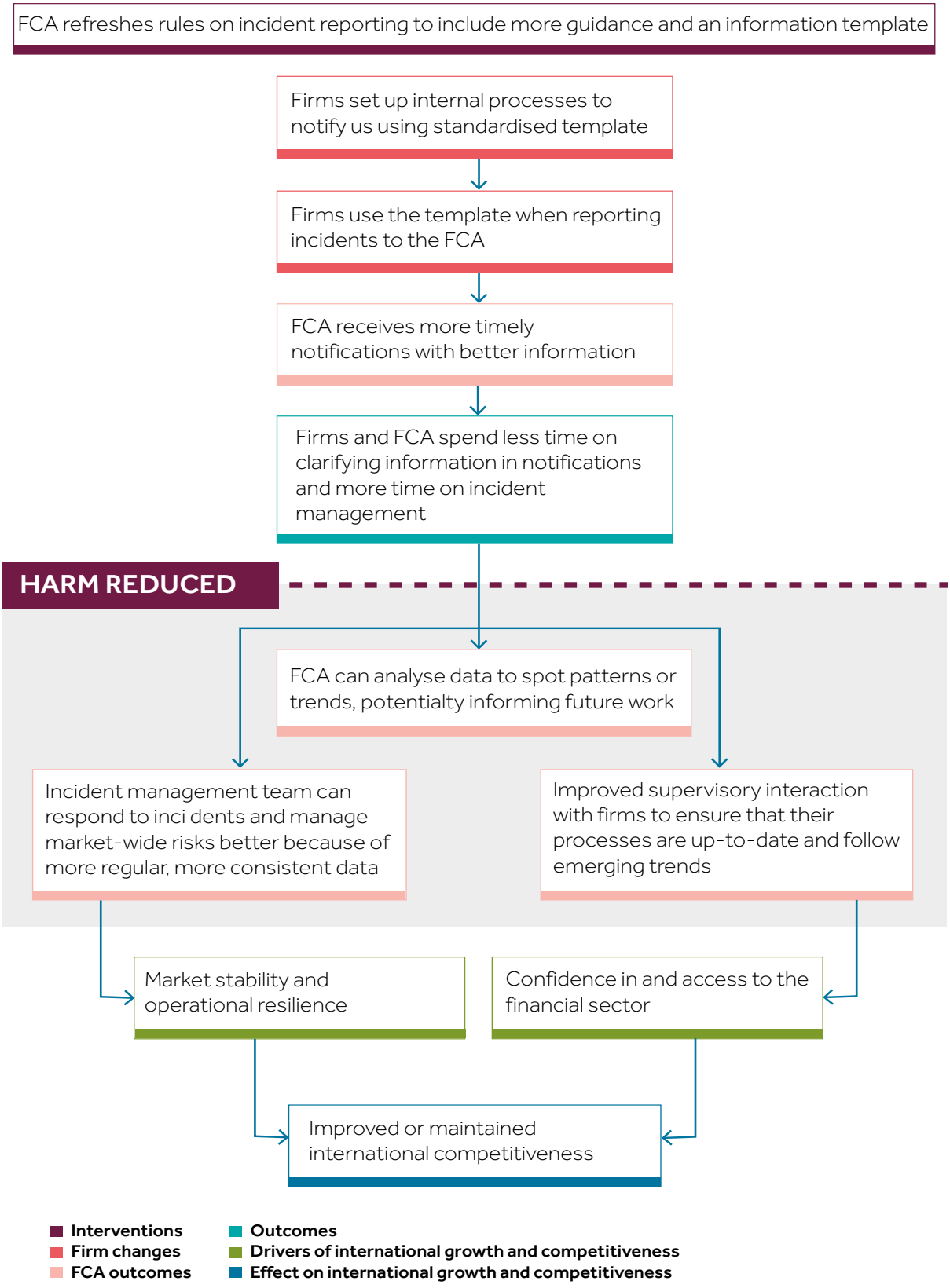
Existing requirements and new proposals	Summary
Existing requirement: relations with regulators	Principle 11 (PRIN 2.1.1R) requires a firm to deal with its regulators in an open and cooperative way, and disclose to us appropriately anything relating to the firm of which that regulator would reasonably expect notice.

Existing requirements and new proposals	Summary
Existing requirement: notification of operational incidents to the FCA	SUP 15.3.1 requires a firm to notify us immediately it becomes aware, or has information which reasonably suggests, that any of the following has occurred, may have occurred or may occur in the foreseeable future: **1.** the firm failing to satisfy one or more of the threshold conditions; or **2.** any matter which could have a significant adverse impact on the firm's reputation; or **3.** any matter which could affect the firm's ability to continue to provide adequate services to consumers and which could result in serious detriment to a firm's consumers; or **4.** any matter in respect of the firm which could result in serious financial consequences to the UK financial system or to other firms.
Proposal: standardised reporting structure and location	*Note – this applies to a firm; a payment service provider, a UK RIE; a trade repository; and a credit rating agency.* Firms in scope are required to use the standardised template for incident reporting, via an electronic portal.
Proposal: additional reporting requirements for in-scope firms	*Note – this applies to a firm; a payment service provider, a UK RIE; a trade repository; and a credit rating agency.* Firms in scope are required to assess the impact of an incident against thresholds aligning with our objectives. They are also required to submit the reports within specific timeframes.

The causal chain

31. The causal chain illustrates how we expect our proposals to reduce harm and the mechanisms through which this will occur.

Figure 3: The incident reporting causal chain



Third Party Reporting

The Market

32. Many firms use technology, platform and cloud related third party provider (TP) arrangements to support important business services. Examples of these arrangements include:

- Purchase of hardware, software, and technology platforms including cloud hosting.
- Use of aggregators or facilitators to access another financial market infrastructure.
- Use of a supply chain for the provision of hardware, and other information, communication, and technology products.

33. Potential risks to UK financial stability and market confidence could arise if a TP fails or suffers a major disruption. Some TPs have a large concentration across the market, and therefore a failure in any one of them can have a large adverse effect on the financial system. As firms' use of TPs increases, so do these associated risks. A report by the European Securities and Markets Authority (ESMA) used a stylised model to measure operational risk and concluded that 'Critical Service Providers need to be significantly more resilient than firms to improve the safety of the financial system'.

34. Consumers may be increasingly aware of this concentration risk, with some recent high-profile disruption such as the CrowdStrike incident in July 2024 affecting many products and services across different sectors, for example healthcare, travel, and finance.

Problem and rationale for intervention

Harm

35. TPs play a growing role in helping firms deliver their important business services. The Bank's Financial Policy Committee (FPC) identified the need to address systemic risks posed by overreliance in the market on a concentration of third parties, which cannot be managed by firms individually. These risks stem from firms' and FMIs growing dependency on third parties for services whose failure or disruption could have a systemic impact on our objectives. They also stem from the concentration in the provision of these services, which can arise from direct contractual arrangements between firms and FMIs, and third parties (and/or indirectly through third parties' supply chains and other forms of interconnectedness).

36. The potential impact of the failure or disruption to these services on the stability of, or market integrity of the UK financial system and the resilience of firms and FMIs.

37. In 2023 we received around 1,000 operational incident reports, of which nearly a quarter were directly or indirectly related to third party providers.

38. Disruption to any material services that certain TPs provide to firms and FMIs could therefore lead to a single-point-of-failure that may simultaneously impact multiple firms and FMIs, consumers, and in extreme cases, UK financial stability.

39. For disruption that originates at a TP which multiple firms rely on, the costs from the incident could be five times higher per incident, as set out in the CBA of the critical third parties regime. This multiplier is based on the PRA's 2021 outsourcing register data, which indicates that up to five firms outsource services to the same TP supplier for the same type of important business service. As such, the cost of an incident to a firm's important business services is multiplied by five to estimate the cost of disruption at a critical third party (CTP) to be £3.4m.

40. The scale of harm will depend on the scale of the operational disruption to the financial sector and can be considerably more than the broad estimate above; past examples can be used to demonstrate the scale of losses to firms and consumers possible when a third party encounters issues (such as a cloud outage) that affect the sector.

41. For example, in 2019, e-money provider Travelex suffered a large data breach where hackers stole consumer information. This was due to their virtual private network having a vulnerability. According to This is Money, Travelex's parent company, Finablr, reported a £25m loss in revenue in their Q1 2020 accounts in the aftermath of the incident, attributed to both the breach and the early stages of Covid-19.

Drivers of harm

42. If firms are not appropriately managing the risks of relying on third parties, there is an increased possibility of harm on a firm-specific basis. However, there is also an increased risk of even more significant harm and disruption across the system. Even if individual firms appropriately address their own third party risks, this alone does not address the systemic risks that arise from a concentration of firms across the markets relying on the same third party.

43. This is further compounded because of poor data visibility. We do not currently require FCA solo regulated firms to maintain and submit a TP register. Instead, the FCA and PRA currently collect data on firm's TP arrangements via voluntary survey submissions from a subset of firms and FMIs.

44. With this reduced dataset it is more difficult for us to assess and manage the systemic risk presented by firms increasingly relying on third parties for their important business services. The lack of a centralised TP database also restricts our ability to assess the true scale and severity of an incident affecting multiple firms dependent on the same third party. Supervisors spend valuable time and resource engaging with firms to establish which firms are affected. A slowed response increases the risk of harm to consumers and markets crystallising.

Options

45. We considered two options to address the harms discussed above. The scope of firms differs in each option, and this is explained in table 3 below.

Table 3: Options assessment for TP

Option	Assessment
All firms to maintain and periodically report material third party arrangements	This option will ensure that we are aware of all material third party arrangements amongst firms. However, this option is not preferred as it may cause undue regulatory burden on smaller firms, and the requirement is not proportionate to the risk.
Firms in scope of the operational resilience policy and CASS large firms to maintain and periodically report material third party arrangements.	This option covers most firms that are strategically important to the integrity of the FS sector and will not increase the regulatory burden on smaller firms. This is the preferred option.

Our proposed intervention

46. We aim to strengthen our existing notification rules around TP risk management within SUP 15 for an estimated 2,200 firms.

47. It is proposed that Board members and Senior Management staff are required to be involved in the governance and oversight of TPs. This will clearly set out our expectations on governance, including under the Senior Managers and Certification Regime (SM&CR), and on record keeping.

48. We will outline detailed TP oversight guidelines to facilitate greater resilience with the adoption of the cloud and other new technologies (FG 16/5 Guidance). Setting out detailed data requirements for the TP register, which includes common data elements (eg, Legal Entity Identifier, FCA permissions) from incident reports which will enable linking of an incident and TP data using analytical tools.

49. We will leverage existing PRA TP register requirements (SS2/21) and where relevant enhancements based on relevant requirements under the European Union's (EU) Digital Operational Resilience Act (DORA). The difference between the current requirements and the new requirements is set out below in Table 4.

Table 4: How our new requirements differ from existing requirements

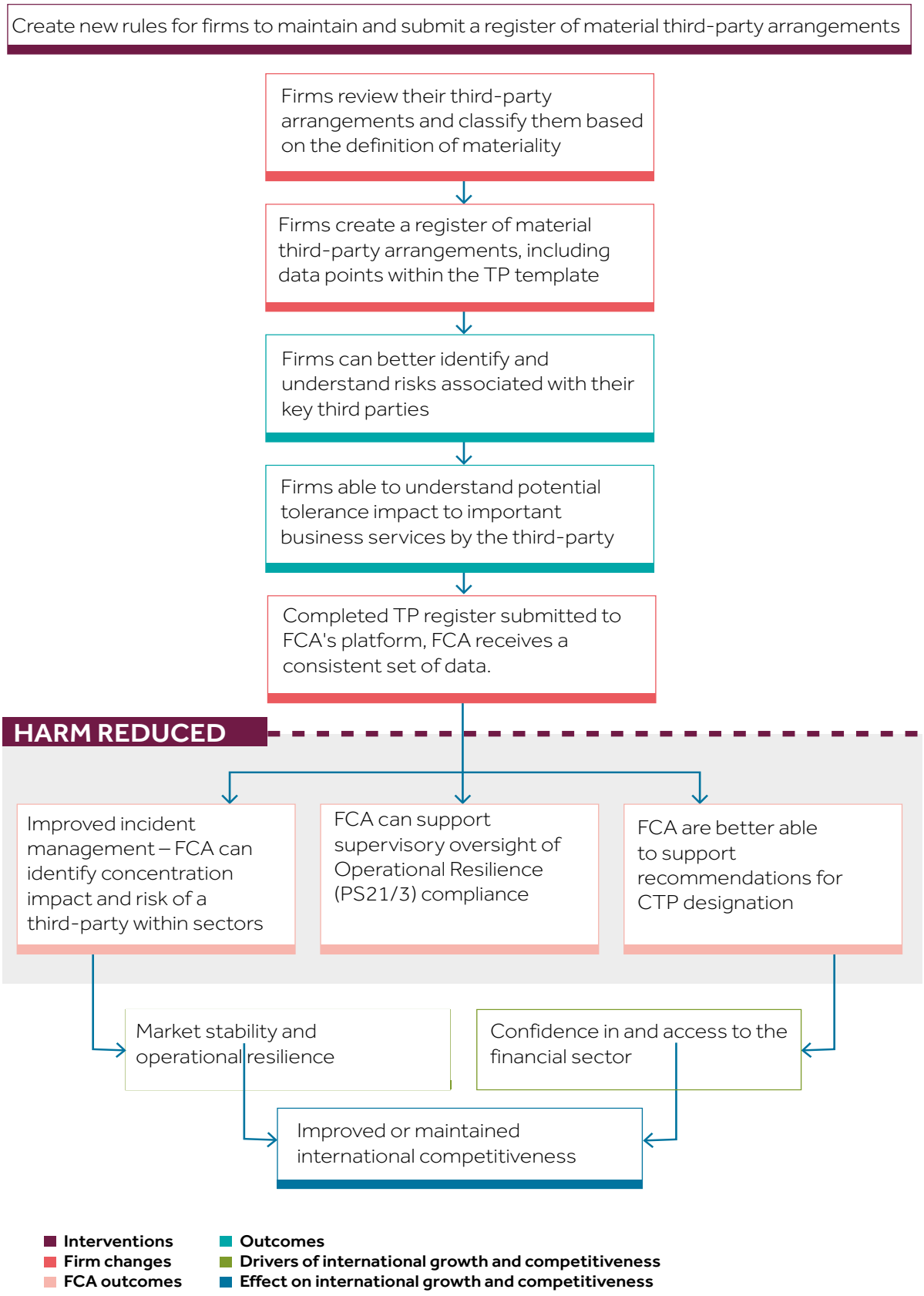
Existing requirements and new proposals	Summary
Existing requirement: relations with regulators	Principle 11 (set out in PRIN 2.1.1R) requires a firm to deal with us in an open and cooperative way, and to disclose to us appropriately anything relating to the firm of which that regulator would reasonably expect notice.
Existing requirement: notification of material outsourcing arrangements to us	SUP 15.3.8(e) requires that firms give us notice of entering into, or significantly changing, a material outsourcing arrangement, as one of the forms of proposed restructuring, reorganisation or business expansion which could have a significant impact on the firm's risk profile or resources.
New proposal: notification on material third party arrangements	*Note – this applies to a select scope of firms. See box 'scope for TP'.* A Firm must give us notice when entering into, or significantly changing, a material third party arrangement, which represents an expansion in scope from only material outsourcing arrangements to both outsourcing and non-outsourcing.
New proposal: Third party register requirements – maintain register	*Note – this applies to a select scope of firms. See box 'scope for TP'.* Firms in scope must maintain a register of information relating to their material third party arrangements. They must submit this information as specified under SUP 16 Annex 17 annually to us by completing the fields online through the appropriate systems accessible from our website.

	Scope for TP:
	• *a firm that is:*
	  ◦ *an enhanced scope Senior Managers & Certification Regime (SMCR) firm;*
	  ◦ *a bank;*
	  ◦ *a PRA designated investment firm;*
	  ◦ *a building society;*
	  ◦ *a Solvency II firm;*
	  ◦ *a CASS large firm;*
	• *a UK recognised investment exchange (RIE);*
	• *an authorised electronic money institution or an authorised payment institution; and*
	• *a consolidated tape provider.*

The causal chain

50. The causal chain illustrates how we expect our proposals to reduce harm and the mechanisms through which this will occur.

Figure 4: The Third Party reporting (TP) causal chain



Appraisal

51. This section sets out our judgement of the expected impacts of both interventions relative to the baseline, including key assumptions that underpin the costs and benefits.

52. Both interventions (incident reporting and third parties) are covered in this section together where relevant. The cost and benefit sections are split with separate headings to denote each intervention.

Baseline

53. There are a number of existing requirements that will continue to apply to firms.

54. Section 15 of the supervision manual ('SUP') in the FCA Handbook requires firms to report matters having a serious regulatory impact. The rules currently give a broad definition of what such a matter could be but are not specific in setting out at what time or for exactly what detail firms should report to us.

55. In 2021 we published PS21/3 setting our final rules on building operational resilience in the UK FS sector. These rules apply to select categories of firms and will be enforceable from March 2025. The requirements are for firms to:

- identify their important business services that if disrupted could cause harm to consumers or market integrity
- identify and document the people, processes, technology, facilities and information that support a firm's important business services (mapping)
- set impact tolerances for each important business service (ie thresholds for maximum tolerable disruption)
- test their ability to remain within their impact tolerances through a range of severe but plausible disruption scenarios
- conduct lessons learned exercises to identify, prioritise and invest in their ability to respond and recover from disruptions as effectively as possible
- develop internal and external communications plans for when important business services are disrupted
- develop internal and external communications plans for when important business services are disrupted

56. These requirements seek to strengthen operational resilience within regulated firms. The improvements they make to operational resilience will allow firms to react faster and more effectively when their important business services are disrupted, thereby reducing the number of consumers affected and lessening the impact on those that are affected.

57. While this operational resilience regime requires firms to adequately manage the risks of their TP arrangements, it does not require firms to maintain and submit a register of them. The regime's other requirements do not elicit an optimal level of detail on TP arrangements needed for purposes such as making recommendations for CTP designation or for better managing third party related incidents. For example, the self-assessment does not require firms to submit a list of the third parties they use or specify which services they rely on the third party for.

58. Finally, in PS7/21 and SS2/21, the PRA set out their requirements for all PRA regulated firms to maintain an internal register of their outsourcing agreements in line with the EBA Outsourcing Guidelines.

59. There are some new and proposed requirements that will also apply to some firms within scope of these proposals.

- The EU has introduced DORA, to be implemented in January 2025. It is likely that firms operating in both the EU and the UK will therefore already have risk registers for outsourcing and third parties set up, though they may not meet all the proposed FCA requirements.
- The PRA is also consulting (concurrently with the FCA) on an online portal where firms will submit data from their outsourcing registers to the PRA. As part of our operational resilience rules set out in PS21/3, firms are required to map their risk involving third parties, however they are not automatically required to send these to us.

60. Left unaddressed, the issues we face with reporting are likely to worsen as regulatory demands on data increase, and as the PRA and FCA strive to become more data driven regulators.

61. Continuing to rely on voluntary manual submission requests of outsourcing relationships hinders our ability to correlate and understand concentration risks across the sector. The absence of rules around technology product, platform and cloud related TP providers means that we will not have visibility of end-to-end TP relationships across solo regulated firms.

62. Because the FS sector is so inter-connected, disruption from one incident at one firm can spread quickly. Firms increasingly use third party providers, believing that the backing of a large company with established IT and cloud systems may increase their own operational resilience, but the more firms that rely on any one third party, the larger the effect of a system-wide incident will be, potentially disrupting market stability.

63. Without TP data, we will struggle to monitor and manage market-wide incidents effectively, which could contribute to increasing the risk of harm to consumers and the wider economy.

Key assumptions

64. The FCA and PRA have worked together to take a proportionate approach to collect evidence from firms. To do this we assumed that the PRA's firm size definition translates to the FCA's as: PRA large or medium are equivalent to FCA large, PRA small is equivalent to FCA medium or small. We also assumed that the expected increase in a firm's number of outsourcing arrangements per year (collected by the PRA using their SS2/21) is used to proxy for the expected growth of material non-outsourcing TP arrangements per year.

65. We assumed that incident notifications are growing at a rate of 6%, the average growth rate between 2018 and 2023. It is possible that following the introduction of these proposals, the true increase in notifications will be larger, but this is not possible to accurately predict.

66. The benefits case relies on our being able to proactively and productively use the data we receive, both in the form of incident reports and third party registers. In order to better manage risks and prevent them from materialising, FCA resource will be needed to maintain, monitor and regularly analyse the gathered data.

67. Throughout the analysis, the daily cost of employing a compliance professional is used to calculate the cost of performing tasks such as reading documents and engaging with us. As set out in Appendix 1 of our Statement of Policy on Cost Benefit Analysis, salaries for large and medium firms are based on the 2022 Willis Towers Watson UK Financial Services Report. Small firm salaries were sourced from a systematic review of adverts on the websites of Indeed, Reed and Glassdoor, which we cross-referenced with other publicly available sources. Salary estimates were uplifted by 7.9% in 2024 and by 7.5% in 2023 using ONS full-time gross earnings figures for the finance and insurance sector. The wage is multiplied by the ONS' non-wage cost multiplier (1.179) to give a full employment cost. Finally, this is divided by the number of working days in a calendar year, assumed to be 220.

68. We assume that once firms are familiar with the new incident reporting rules and use of the notification template, there are no new ongoing (annual) costs. This is because firms are already expected to notify us of material operational incidents.

69. Because both proposals (incident reporting and third parties) seek to change the way firms notify us of incidents or register non-outsourcing third party relationships, we do not expect any additional costs to fall on third parties. It is expected that firms should already hold enough information on the third parties they have arrangements with to fill out the register.

70. Consistent with the HM Treasury Green Book, the impacts are assessed over a 10 year appraisal period and a discount rate of 3.5% is applied to estimate present value stream of costs and benefits over the appraisal period.

71. All costs are expressed in 2024 prices unless otherwise stated.

Summary of Impacts

72. The proposals will support operational resilience in the financial system as we can more efficiently respond to third party concentration risks and firms affected by operational incidents.

73. Firstly, more timely and consistent information on incidents will enable us to assess and respond to operational incidents at firms and their associated risks to the financial sector in a more timely, proportionate, and informed manner. This can result in reduced harm to market participants, for example, significant financial losses.

74. Firms are likely to save some time spent in follow-up with us after an incident notification is submitted as firms will be required to provide all the required information at the outset, reducing follow-up conversations. This efficiency benefit is estimated to be £2.90m (present value) in total over the 10 year appraisal period. With less time spent

on reporting and more spent on addressing an incident together, harm arising from an incident could be reduced, meaning that both the FCA and firms benefit from increased operational resilience.

75. Secondly, market participants will benefit from improved third party reporting that can enable us to identify third party risks quicker, by identifying other affected firms using the submitted register data.

76. Across all in-scope firms, compliance costs are the most substantial cost element. We estimate the cost of compliance using our standardised cost model (SCM). More detail on the SCM, including why it is used, can be found in our Statement of Policy on Cost Benefit Analysis.

77. Cost estimates vary by firm size and business type, though the average cost per firm associated with these proposals is likely to be small. Firms in scope of both IR and TP are larger on average, and it is this group that face a higher cost.

78. We estimate the total one-off costs for familiarisation and gap analysis to firms are £12.63m (£11m attributed to the firms in scope of only IR, and £1.63m attributed to firms in scope of both IR and TP). Firms in scope of TP reporting face an additional one-off cost for setting up the material third party register, which is estimated to be between £6.51m and £14.08m. Finally, firms in scope of TP proposals are estimated to face an annual ongoing cost of between £36k – £116k for updating their TP register with additional arrangements on an annual basis (per firm estimates are listed in Table 12).

79. The main benefits and costs are summarised in Tables 5 to 7 below.

Table 5: Summary of benefits and costs

	Benefits		Costs	
Impact	One off	Ongoing (annual)	One off	Ongoing (annual)
All in-scope firms (c.41,500)				
Familiarisation cost & gap analysis (direct)			£12.63m	
Third Party Reporting (c.2,200 firms)				
Setting up a new TP register (direct)			£6.51m – £14.08m	
Adding new arrangements to the register (direct)				£0.04m – £0.12m
Reduced harm to market participants from improved monitoring of TP risks by FCA (indirect)		Minimal (not quantified)		

Impact	Benefits		Costs	
	One off	Ongoing (annual)	One off	Ongoing (annual)
Incident Reporting (c.41,500)				
Reducing time spent in follow-up with the regulators (direct)		£0.27m		
Reduced harm to market participants from faster intervention and management of incidents (indirect)		Minimal (not quantified)		
Total		**£0.27m**	**£19.14m – £26.71**	**£0.04m – £0.12m**

Table 6: Present Value and Net Present Value across 10 year appraisal period

	PV Benefits	PV Costs	NPV
Total impact	£2.90m	£19.41m – £27.59m	(£16.51m – £24.69m)
– of which direct	£2.90m	£19.41m – £27.59m	(£16.51m – £24.69m)
– of which indirect	–		–

Table 7: Net direct costs to firms

	Total (Present Value) Net Direct Cost to Business (10 years)	Equivalent Annual Net Direct Cost to Business (EANDCB)
Total net direct cost to business	(£16.51m – £24.69m)	(£1.92m – £2.87m)

80. Whilst there is an increase in regulatory burden due to the proposals, we consider this is proportionate to the scale of systemic risks posed by increasing concentration of the use of some third parties and the scale of harm from operational incidents as set out in the Harms section. Therefore, any small improvement to the reporting process could help to offset those costs.

81. Although the net present value is negative, we expect that the benefits can be higher than the costs of these proposals, because the non-quantified benefits could be substantial. It is not possible to reasonably estimate the exact loss or disruption that may be prevented as there is no way of predicting future incidents and their scale. However, improved reporting data and processes give us better visibility, enabling firms and the FCA to identify and address risks earlier, and potentially more effectively. This should ensure that incidents' severity is minimised, and they are managed more rapidly. Our ability to use better reporting data and processes to minimise harm will depend on the circumstances of the incidents and concentration risks third parties pose.

Benefits

Benefits to market participants (firms and consumers)

Incident Reporting

82. Firms will directly benefit by providing required information for an incident report at the outset, reducing follow-up exchanges with the regulator. This is because the new reporting template and updated guidance will clearly set out what information is required. Compliance staff time in firms that will otherwise have been used in such engagement can be allocated to other tasks related to dealing with incidents, which could help to reduce losses and harm.

83. Based on our outreach to firms, set out in detail in the costs section, the mean working time spent in follow-up with the regulators after submission of an incident report is 1.35 FTE staff days. However, many firms told us that more complex incidents often require over a week of follow-up conversations with the regulators to provide further information. Because complex incidents are more likely to cause harm, it is important that firms can focus their time on dealing with the incident as it arises, which reducing the regulatory burden can contribute to.

84. Through supervisory insight it is estimated that by using our template, firms will spend 50% less of the mean FTE spent in follow-up reported to us. In sum, we estimate a benefit of £240 – £260 per incident, depending on firm size. In order to capture the growth in expected number of incidents reported, we apply the mean growth in reports from 2018-2023 (6% p.a.) to each subsequent year of the appraisal period. This gives a total 10-year present value benefit of £2.90m.

85. Because firms may need to take some time to adapt to using the incident reporting template, we fully offset the year one benefit of reduced time spent in follow up. It is not possible to directly quantify this cost, but it is likely that some firms may still require a follow-up conversation with us, particularly in more complex cases.

86. As set out in the Harms section, the scale of losses caused by incidents can be large.

87. Consumers and market participants will indirectly benefit from improved incident reporting because we will be able to act sooner in the event of material incidents and third party disruptions to minimise harm. We may also be able to use the data gathered to enable future work seeking to prevent consumer harm and market disruption.

88. Therefore, any small improvement to the reporting process could help to offset those costs, whether the improvements allow us to monitor market-wide risks better or simply allow us to support firms to manage incidents faster.

Third Party Reporting

89. The proposals will help to improve firms' operational resilience, which benefits firms as the shocks and spread of third party incidents will be better managed. The resulting data will allow us to proactively reach out to firms in instances where one or some firms identify an issue with a third party, but other firms may not be aware of the issue even though they rely on the affected third party. This may allow those firms to take preventative measures to prepare for their services being affected.

90. The submitted registers will also be used to help us inform our recommendations of third parties to HMT for designation as CTPs. A consistently formatted, updated dataset will facilitate the identification of where many firms rely on the same TP. The ability to identify new CTPs will contribute continued benefits of enhanced operational resilience and management of operational incidents at CTPs as outlined in CP23/30.

91. As third party disruption often causes widespread financial losses, it can ultimately lead to consumers experiencing financial loss or loss in confidence in the financial system. Market participants will therefore benefit from improved third party reporting that can enable us to identify third party risks quicker, and intervene and manage the risks of an incident at a third party to the financial sector more effectively.

Benefits to the FCA

92. The quality and usability of incident data received will be enhanced by the template that firms will need to use to report incidents. We can use this data for thematic analysis and horizon scanning to identify emerging operational and cyber resilience risks to the FS sector. By stipulating timings for reporting incidents, our incident management team can take the appropriate regulatory actions to manage risks to consumers and markets in a timely manner.

93. Reduced follow-up time spent engaging with firms to gather more information will also help this. When a firm reports an incident, our incident management team must manually assess the report to understand if any additional information is needed. They must then engage with firms to gather the missing information. This opportunity benefit provides a chance for the incident management team to focus their resource on the management of emerging incidents, instead of on gathering further data from firms.

94. Additionally, we will be able to use the consistent dataset on TP arrangements to inform assessments of firms' resilience to third party incidents. Connections can be made at a firm level to a given TP, ensuring that in the event of an incident, we can assess which other firms we might expect to be affected. This should contribute to timely incident management, reducing the time in which impacts like financial losses can accrue.

95. There is potential for benefits to the financial sector and the wider economy arising from our use of reported data. This may take the form of identification of broader themes in the data to inform future regulatory work, or by improving our ability to respond to material incidents, which could reduce the associated impact.

Costs

Costs to firms

Familiarisation costs and gap analysis

96. Firms will incur costs to familiarise themselves with the requirements and complete a gap analysis to understand what they need to do to meet the updated requirements.

97. We have used our SCM to estimate the cost to firms to familiarise themselves with the proposals and complete gap analysis. We assume that costs occur to firms according to their size in the SCM, as defined using fee-block data (see page 42 of our Statement of Policy on cost benefit analysis for more details).

98. The daily labour cost of a member of compliance staff is estimated to be between £350 and £390 depending on the size of the firm, including salary (from our SCM) and a non-wage labour cost uplift. This is then adjusted for the time taken to read the CP and legal documentation.

99. Firms in scope of IR rules will be required to read 63 pages of the CP and 5 pages of legal documentation. Firms in scope of both IR and TP proposals will be required to read all 79 pages of the consultation paper and 14 pages of legal text. We assume that between 1.5 and 6 FTE staff will be required to read the CP (excluding the instrument). We also assume that the legal team reviewing legal documentation will be between 1.5 and 3 FTE staff. The total estimated costs from familiarisation and gap analysis per firm and in total are set out in table 8 below.

Table 8: Costs due to familiarisation and gap analysis

Scope	Size	Per firm cost	Total cost
IR only (c.39,000 firms)	Large	£1,470	£122,000
	Medium	£850	£740,000
	Small	£260	£10,143,000
	Total	–	£11,005,000
IR and TP (c.2,200 firms)	Large	£2,050	£363,000
	Medium	£1,120	£750,000
	Small	£350	£516,000
	Total	–	£1,628,000
	Grand total	**–**	**£12,634,000**

Note: per firm costs are rounded to the nearest £10. These may not sum exactly to the total costs, which are rounded to the nearest £1,000.

Incident reporting costs

100. We do not expect firms to face any additional costs due to the proposals in addition to familiarisation and gap analysis costs as they already submit incident notifications and provide necessary information through follow-up engagement with us. However, to consider the scale of burden from submitting an incident report, we have sought to estimate the cost of submitting an incident report using the current rules and process.

101. The current incident reporting process involves a firm gathering data, whether manually or using an automated system, before formatting this into an email and sending it using FCA Connect. We may seek to gather further information by reaching out to the firm through follow-up engagement.

102. To inform policy development, we selected a random sample of solo-regulated firms, defined as small in our SCM, which have reported incidents to us since 2021. Fifty-seven firms were sampled, with 46 responding to us within 3 weeks. This sample was asked a set of questions on the FTE days used to complete the incident reporting process, listed in Table 9 below alongside the corresponding average (mean) FTE answer from respondents.

Table 9: FCA outreach questions and average FTE responses

Question	Mean FTE days
How much time does it usually take to log the information of an incident into the firm's internal incident management systems?	0.45
How much time is usually needed to complete an incident notification to the FCA under the General Notification requirements?	1.02
How much time is needed to complete the notification process by putting the information into a submittable format for the FCA (eg, an email)?	0.79
How much time do you typically spend on follow-up conversations with FCA (phone calls and email exchanges) after the initial submission of the incident notification?	1.35

103. Firms were also asked whether they have an automated incident management process and if so, what the effort to build it was. Responses to this question were mostly not answered in FTE, but one-third of the firms which responded said they had a semi- or fully- automated incident management system, some built internally but most procured by software companies.

104. The PRA also sampled a selection of their firms, asking about their material arrangements to inform cost estimates. The questions on material outsourcing notifications, and the corresponding average (mean) FTE provided by respondents, are presented in Table 10, split by PRA firm size.

Table 10: PRA IR outreach questions and average FTE responses, by firm size

Question	Average FTE days		
	Large	Medium	Small
How much time does it usually take to log the information of an incident into the firm's internal incident management systems?	0.77	0.69	0.80
How much time is usually needed to complete an incident notification to the PRA under the Notifications Parts 2.1(3)?	1.46	1.44	2.27
Reflecting on the previous question, how much time is needed to complete the notification process is used for putting information into a submittable format (eg, into an email)?	0.44	0.41	1.08
How much time do you typically spend on follow-up conversations with PRA (phone calls and email exchanges) after the initial submission of the Notification?	0.36	2.09	2.51

105. Using the SCM in conjunction with the FTE estimates from the firm outreach, the total cost of submitting an incident report to us is approximately £1,000. This is the total of the FTE reported to us for a firm to log incident information internally, format that information for us and provide follow-up information as requested.

106. It is acknowledged that there may currently be a level of underreporting. Therefore, the total cost to all firms is lower than expected. Should the proposals cause an increase in incident notifications, it is likely that more firms will incur the cost of submitting a notification. It is not possible to estimate any potential increase in notifications, because the scale of underreporting is unknown.

107. The proposals will introduce a template with more guidance and clarified fields of information for firms to fill in, ideally saving time in the follow-up interaction. The information needed to form an incident report remains the same, but this will be clearly set out in the template, meaning that instead of gathering it in two stages (initial report and follow up) it is all gathered for the initial report.

108. There is however likely to be a period of adjustment where firms must adapt their existing processes to gather all of the information for the initial report. This is instead of the current process of gathering what they can, submitting it, and engaging with the regulators in follow-up to collect further information. To account for this, the efficiency benefit arising from reduced follow-up time is offset by an equivalent one-off cost in year one.

TP costs

109. Firms will face an up-front cost of setting up a material third party register. They will then face an ongoing cost to update the register with new arrangements annually.

110. The PRA asked a selection of 44 firms questions regarding their 2023 Outsourcing Register trial, where firms were asked to maintain and submit a register of material outsourcing notifications. 35 firms responded. The questions and corresponding mean FTE responses are presented in Table 11. Across all 35 respondents to the PRA's outreach, the average one-off FTE required to set up the register is 31 FTE days.

Table 11: PRA TP outreach questions and average FTE responses, by size

	Average FTE days		
Question	Large	Medium	Small
In relation to the end June 2023 Outsourcing Register data collection, how much time was required to complete the submission process?	28.28	16.14	4.59
Did your firm require any technology enhancements to assist in the completion and submission of the Register? If so, what was the estimated FTE effort requirement?	27.81	0 (No tech)	24.80

111. We also asked a sample of firms to report the anticipated financial cost of setting up this register. Five firms responded with FTE days or cost estimates, which fell broadly into the ranges given by respondents to the PRA.

112. We used the PRA's outreach responses to estimate the costs of the TP proposals. This is because the PRA's sample of responses was higher with 35 respondents, making their estimates more representative.

113. We map the costs such that the PRA-defined large and medium estimates are used to estimate the costs for FCA-defined (as per our SCM) large firms, and the PRA's small-defined estimates map to FCA-defined medium and small firms. Firms regulated by the PRA are, on average, larger than those regulated by us. Although having equal estimates for both small and medium firms may result in an overestimation of cost, the ranges are similar.

114. Some firms in scope of the TP proposals may have an existing register to record third party arrangements. For the purposes of this analysis, the cost of adapting an existing register is not calculated. Instead, the cost of building a new register is applied to all firms. This means the costs are slightly overstated, however it is not possible to accurately reflect the varying levels of existing technology in a calculation of the cost of adapting the register.

115. Once a firm has a register, it is required to ensure it is up to date every year. Therefore, from year two onwards, firms face a small ongoing cost in adding any new material arrangements to their register. PRA analysis shows that across all firms, there are an average of 4 additions to registers per year. We assume that this proportion can be a proxy for the proportion of firms who will increase the number of material non-outsourcing notifications in a given year.

116. The PRA, using their outreach responses, estimate the total annual FTE effort for maintaining the register as between 0.04 – 0.08 for small firms, 0.09 – 0.45 for medium firms, and 0.19 – 2.01 for large firms. We multiply this by the daily employment cost of a compliance professional to obtain monetary costs.

117. Based on this analysis, the costs of the TP proposals estimated are in Table 12 below.

Table 12: TP Reporting Costs to firms

Cost	Size	Per firm cost	Total cost
Setting up the register (one-off)	Large	£3,200 – £28,300	£460,000 – £3,420,000
	Medium	£3,000 – £5,200	£1,890,000 – £3,310,000
	Small	£3,000 – £5,200	£4,160,000 – £7,340,000
	Total one-off cost		£6,510,000 – £14,080,000
Adding new arrangements to the register (annual cost from year two onwards)	Large	£60 – £480	£6,800 – £58,100
	Medium	£10 – £30	£9,000 – £18,000
	Small	£10 – £30	£20,000 – £39,900
	Total ongoing (annual) cost		£36,000 – £116,000

Note: Costs are rounded to the nearest £100, except where they are less than £1,000.

Costs to the FCA

118. As part of these proposals, we will create a new incident notification template and a template for material non-outsourcing arrangements register. The cost of creating these templates is covered by existing departmental budget and resource.

119. It is expected that 2 FTE staff will join the existing incident management team of 5 FTE staff to increase our ability to handle the caseload of incident notifications and manage incidents with firms.

120. We also plan to recruit 2 FTE data analysts to process and manage the submitted third party registers which we receive from firms. Other roles may in future be created to analyse the data for emerging risks and trends, which will help us identify CTPs for designation and improve our response capabilities.

Wider economic impacts, including on secondary objective

121. We believe that the impact of these proposals will neither materially affect the international competitiveness of the UK economy, nor its growth in the medium to long term.

122. The IR proposals build on existing rules in the FCA Handbook. Because we already have rules in place which mandate incident reporting, the proposals will have a small impact on firms. The proposals may have a small positive impact to growth of the wider economy and international competitiveness, arising from increased stability and transparency.

123. The TP proposals are new to FCA-regulated firms. However, the EU is implementing DORA, and the PRA already requires firms to submit third party registers. The proposals align the two regulators and increase alignment with the EU. In the long-term as consumer confidence increases, we believe that the proposals may enhance international competitiveness and the wider growth of the UK economy, making its financial system more resilient to damaging shocks.

Monitoring and evaluation

124. Table 13 sets out the outcomes we expect from these proposals and the mechanisms through which we expect the proposals to deliver these outcomes.

125. We will review, and, if necessary, update both the IR template and TP reporting template on an annual basis.

Table 13: Measuring the success of the proposals

Outcomes	Mechanisms	How will we measure success?
Incident reporting		
A wider pool of firms which report incidents	Clear guidance and a prescribed template so that firms can submit all the required information to us when the incident is first reported.	We will monitor incident reporting data to look for sector and portfolio reporting patterns.
Less time taken for a firm to report an incident upon discovery, meaning we can work with firms at an earlier stage and manage the impact of incidents.	Specifying times at which firms should report in our rules and clarifying expectations.	The difference between the 'incident date' and 'date reported' fields in the template will be used to measure the average time taken. Further, we can provide insights into changes to their work.
Increased volume of complete Post Incident Reports (PIR) received. This will allow us to perform thematic analysis of incident root causes.	More timely incident reports allow firms work with us to manage the impacts more efficiently; firms will have a more complete information set to provide a completed PIR.	The number of completed PIRs per incident reported will be monitored to measure whether more incidents yield a completed PIR at their closure.
Third Party Reporting		
Greater percentage of CTPs being recommended for designation from the TP data collection.	The submission of the new register will allow us to quantitatively support supervisory insight when making recommendations.	We will monitor the number of CTPs designated using a combination of supervisory input and TP register data.

Outcomes	Mechanisms	How will we measure success?
The receipt of consistent data which is rarely rejected (and sent back for further input by a firm) in the TP register.	The provision of an optional template for firms to use when submitting their register will provide clarity of our expectations.	We will monitor the number of submissions which are rejected.
Reduced time spent by FCA obtaining further information from firms, at the start of an incident or when supervisors are monitoring TP risks.	Because we will know, from the register, which third parties are used by which firms, we will not have to spend time gathering this information in the initial stages of a TP incident or during supervisory work.	We will monitor inbox traffic following the report of a TP incident or when supervisors are evaluating a firm's TP risk, with less back-and-forth communication expected.

Annex 3

Compatibility statement

Compliance with legal requirements

1. This Annex records the FCA's compliance with a number of legal requirements applicable to the proposals in this consultation, including an explanation of our reasons for concluding that our proposals in this consultation are compatible with certain requirements under the Financial Services and Markets Act 2000 (FSMA).

2. When consulting on new rules, we are required by section 138I(2)(d) FSMA to include an explanation of why it believes making the proposed rules is (a) compatible with our general duty, under s. 1B(1) FSMA, so far as reasonably possible, to act in a way which is compatible with our strategic objective and advances one or more of our operational objectives, and (b) our general duty under s. 1B(5)(a) FSMA to have regard to the regulatory principles in s. 3B FSMA.

3. We are also required by s. 138K(2) FSMA to state our opinion on whether the proposed rules will have a significantly different impact on mutual societies as opposed to other authorised persons.

4. This Annex also sets out our view of how the proposed rules are compatible with the duty to discharge our general functions (which include rule-making) in a way which promotes effective competition in the interests of consumers (s. 1B(4)). This duty applies in so far as promoting competition is compatible with advancing our consumer protection and/or integrity objectives.

5. In addition, this Annex explains how we have considered the recommendations made by the Treasury under s. 1JA FSMA about aspects of the economic policy of His Majesty's Government to which we should have regard in connection with our general duties.

6. This Annex includes our assessment of the equality and diversity implications of these proposals.

7. Under the Legislative and Regulatory Reform Act 2006 (LRRA) the FCA is subject to requirements to have regard to a number of high-level 'Principles' in the exercise of some of our regulatory functions and to have regard to a 'Regulators' Code' when determining general policies and principles and giving general guidance (but not when exercising other legislative functions like making rules). This Annex sets out how we have complied with requirements under the LRRA.

The FCA's objectives and regulatory principles: Compatibility statement

8. The proposals set out in this consultation are primarily intended to advance our operational objectives of reducing harm to consumers and enhancing market integrity.

9. The proposals will provide clarity on how firms report incidents and material third party arrangements, improving our visibility on firms' operational resilience and third party concentration risks. This supports our supervision and intervention on operational risks and incidents, and identification of potential CTPs.

10. In preparing the proposals set out in this consultation, we have had regard to the regulatory principles set out in s. 3B FSMA.

The need to use our resources in the most efficient and economic way

11. Our proposals are designed to be as proportionate as possible and ensure that our expectations are clear to firms. The information received from firms under the proposals will give us a better understanding of firms' operational resilience and material third party arrangements. This will make our firm supervision more effective and help us better understand and address third party risks like potential CTPs.

The principle that a burden or restriction should be proportionate to the benefits

12. The CBA in Annex 2 sets out the costs and benefits of our proposals. We believe that the benefits of these proposals outweigh the costs.

The need to contribute towards achieving compliance by the Secretary of State with section 1 of the Climate Change Act 2008 (UK net zero emissions target) and section 5 of the Environment Act 2021 (environmental targets)

13. While we do not expect the exercise of this function to be relevant to the making of such a contribution, we have kept this need in mind and will continue to engage with industry and other stakeholders on this during the consultation process.

The desirability of sustainable growth in the economy of the United Kingdom in the medium or long term

14. These proposals support the UK financial sector's operational resilience through providing clarity in incident and third party reporting, which is intended to have a positive impact on firms' ability to recover from operational disruptions and our ability to respond to them. This will contribute to the proper functioning of markets that consumers and firms rely on, which supports growth by helping to maintain the UK as an attractive place to do business.

The general principle that consumers should take responsibility for their decisions

15. The proposals provide clarity on how firms should report incidents and notify us of material third party arrangements. The principle is not engaged because the proposals do not relate to consumer decisions.

The responsibilities of senior management

16. The proposals provide clarity on how firms and senior management fulfil their existing responsibilities under Principle 11 and SUP15.3 General Notification Requirements.

The desirability of recognising differences in the nature of, and objectives of, businesses carried on by different persons including mutual societies and other kinds of business organisation

17. We believe our proposals do not undermine this principle, and that we have appropriately had regard to the variety of firms affected by tailoring them to different firm types.

The principle that we should exercise our functions as transparently as possible

18. We continue to engage with industry and other stakeholders to obtain feedback during the consultation process.

Expected effect on mutual societies

19. The FCA does not expect the proposals in this paper to have a significantly different impact on mutual societies. Only Building Societies and large Friendly Societies covered by Solvency II are in scope of the policy framework.

Compatibility with the duty to promote effective competition in the interests of consumers

20. In preparing the proposals in this consultation, we have had regard to our duty to promote effective competition in the interests of consumers.

21. We consider that consumers may be more likely to choose firms that are more resilient to operational disruptions and that this may drive firms to compete for, and retain, consumers by improving their operational resilience.

22. We have also kept the competition objective in mind when framing how these proposals should be implemented, with a particular focus on whether there is a risk of weakening competitive pressure, disadvantaging smaller firms and potential new entrants.

Equality and diversity

23. We are required under the Equality Act 2010 in exercising our functions to 'have due regard' to the need to eliminate discrimination, harassment, victimisation and any other conduct prohibited by or under the Act, advance equality of opportunity between persons who share a relevant protected characteristic and those who do not, to and foster good relations between people who share a protected characteristic and those who do not.

24. As part of this, we ensure the equality and diversity implications of any new policy proposals are considered. The outcome of our consideration in relation to these matters in this case is stated in paragraph 2.27 of the Consultation Paper.

Legislative and Regulatory Reform Act 2006 (LRRA)

25. We have had regard to the principles in the LRRA for the parts of the proposals that consist of general policies, principles or guidance and consider that the proposals will help firms understand and meet existing and proposed incident reporting and third party reporting requirements, leading to better outcomes for consumers and market integrity. We also believe the proposals are proportionate and take account of the variety of firms in scope.

26. We have had regard to the Regulators' Code for the parts of the proposals that consist of general policies, principles or guidance and consider that the proposals are proportionate and do not create an unnecessary burden on firms, or adversely affect competition.

HM Treasury recommendations about economic policy

27. The HM Treasury recommendations most relevant to our proposals, specifically on the government's economic policy, are:

- growing the financial services sector and increasing its international competitiveness, while enhancing its role in financing growth, safeguarding financial stability and consumer protection, and supporting the transition to a net zero economy
- aspects of the government's economic policy on maintaining and enhancing the UK's position as a world-leading global finance hub and a destination of choice for international financial services business

28. Our proposals aim to clarify how firms should report incidents and third party arrangements. This gives us more visibility on the operational resilience of the UK financial sector and enables more effective oversight of third party concentration risks across the sector. Both enable better outcomes for all consumers, supporting the government's priority to promote its growth and international competitiveness.

29. We believe that our proposals support the Treasury's recommendations on international competitiveness of the UK, as the proposed reporting requirements are aligned with international requirements to allow for more efficient reporting by financial service firms.

Annex 4

Abbreviations used in this paper

Abbreviation	Description
AI	Artificial Intelligence
CASS	Client Assets Sourcebook
CBA	Cost Benefit Analysis
COND	Threshold Conditions
CP	Consultation Paper
CTP	Critical Third Party
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EU	European Union
FCA	Financial Conduct Authority
FIRE	Format for Incident Reporting Exchange
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
FSMA	Financial Services and Markets Act 2000
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IT	Information Technology
LEI	Legal Entity Identifier
NOTP	Non-outsourcing Third Party
OMS	Order Management System

Abbreviation	Description
PRA	Prudential Regulation Authority
PRIN	Principles of Business
PS	Policy Statement
PSD2	Revised Payment Services Directive
RIE	Recognised Investment Exchanges
SM&CR	Senior Managers & Certification Regime
SUP	Supervision Manual (Handbook)
SYSC	Senior Management Arrangements, Systems and Controls (Handbook)
UK	United Kingdom

Appendix 1

Draft Handbook text

NOTIFICATION OF THIRD PARTY ARRANGEMENTS AND OPERATIONAL INCIDENT REPORTING INSTRUMENT 202X

Powers exercised

A. The Financial Conduct Authority ("the FCA") makes this instrument in the exercise of the following powers and related provisions in or under:

(1) the following sections of the Financial Services and Markets Act 2000 ("the Act"), including as applied by paragraph 3 of Schedule 6 of the Payment Services Regulations 2017 (SI 2017/752) ("the PSRs") and paragraph 2A of Schedule 3 to the Electronic Money Regulations 2011 (SI 2011/99) ("the EMRs"):

(a) section 137A (The FCA's general rule-making power); and
(b) section 137T (General supplementary powers);

(2) the following sections of the Act:

(a) section 139A (Power of the FCA to give guidance);
(b) section 293 (Notification requirements); and
(c) section 300H (Rules relating to investment exchanges and data reporting service providers);

(3) the following regulations of the PSRs:

(a) regulation 99(2) (Incident reporting); and
(b) regulation 120 (Guidance);

(4) regulation 60 (Guidance) of the EMRs;

(5) the following regulations of the Credit Rating Agencies (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/266):

(a) regulation 3 (Rules); and
(b) regulation 5 (Guidance);

(6) regulation 74 of the Over the Counter Derivatives, Central Counterparties and Trade Repositories (Amendment, etc., and Transitional Provision) (EU Exit) Regulations 2019 (SI 2019/335); and

(7) regulation 35 of the Transparency of Securities Financing Transactions and of Reuse (Amendment) (EU Exit) Regulations 2019 (SI 2019/542).

B. The rule-making powers listed above are specified for the purpose of section 138G(2) (Rule-making instruments) of the Act.

Commencement

C. This instrument comes into force on [*date*].

Amendments to the Handbook

D. The modules of the FCA's Handbook of rules and guidance listed in column (1) below are amended in accordance with the Annexes to this instrument listed in column (2) below:

(1)	(2)
Glossary of definitions	Annex A
Senior Management Arrangements, Systems and Controls sourcebook (SYSC)	Annex B
Supervision manual (SUP)	Annex C

Notes

E. In the Annexes to this instrument, the notes (indicated by "*Editor's note*:") are included for the convenience of readers but do not form part of the legislative text.

Citation

F. This instrument may be cited as the Notification of Third Party Arrangements and Operational Incident Reporting Instrument 202X.

By order of the Board
[*date*]

Annex A

Amendments to the Glossary of definitions

In this Annex, underlining indicates new text and striking through indicates deleted text, unless otherwise stated.

Insert the following new definitions in the appropriate alphabetical position. The text is not underlined.

material third party arrangement	means 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 *firm* could: (a) cause intolerable levels of harm to the *firm's clients*; (b) pose a risk to the soundness, stability, resilience, confidence or integrity of the *UK financial system*; or (c) cast serious doubt on the *firm's* ability to satisfy the *threshold conditions*, or meet its obligations under the *Principles*, or under *SYSC* 15A (Operational resilience).
operational incident	means either a single event or a series of linked events which disrupts the *firm's* operations such that it: (a) disrupts the delivery of a service to the *firm's client* or a user external to the *firm*; or (b) impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to the *firm's client* or a user external to the *firm*.
registered credit rating agency	means a *credit rating agency* that is registered with the *FCA* under article 14 of the *CRA Regulation*.
registered trade repository	means a *trade repository* that is registered with the *FCA* under article 55 of the *EMIR* or article 5 of the *UK SFTR*.
third party arrangement	means an arrangement of any form between a *firm* and a service provider, whether or not the product or service is: (a) one which would otherwise be provided by the *firm* itself; (b) provided directly or by a sub-contractor; or (c) provided by a *person* within the same *group* as the *firm*.

Amend the following definition as shown.

working day	(1)	(in *PRR* and *MAR* 9) (as defined in section 103 of the *Act*) any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the *United Kingdom*.
	(2)	[deleted]
	(3)	(in *FEES* 9, ~~and~~ *COBS* 19.11 and *SUP* 15.18) any day other than a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the *United Kingdom*.

Annex B

Amendments to the Senior Management Arrangements, Systems and Controls sourcebook (SYSC)

In this Annex, underlining indicates new text.

8 Outsourcing

8.1 General outsourcing requirements

…

General requirements

…

8.1.12 G …

8.1.12A G A *firm* which falls within the scope of *SUP* 15.19 should notify the *FCA* of any new, or any significant changes to, *material third party arrangements*, which include *material outsourcing* arrangements, as set out in that section.

…

13 Operational risk: systems and controls for insurers

…

13.9 Outsourcing

…

13.9.2 G *Firms* should take particular care to manage *material outsourcing* arrangements and, as *SUP* 15.3.8G(1)(e) explains, a *firm* should notify the *FCA* when it intends to enter into a *material outsourcing* arrangement. A *firm* which falls within the scope of *SUP* 15.19 should notify the *FCA* of any new, or any significant changes to, *material third party arrangements*, which include *material outsourcing* arrangements, as set out in that section.

…

Annex C

Amendments to the Supervision manual (SUP)

In this Annex, underlining indicates new text and striking through indicates deleted text, unless otherwise stated.

15 Notifications to the FCA

15.1 Application

Who?

15.1.1 G This chapter applies to every *firm* except that:

(1) only *SUP* 15.10 applies to an *ICVC*; ~~and~~

(2) *SUP* 15.3.22D to *SUP* 15.3.25D apply only to the *Society*~~.~~; and

(3) *SUP* 15.19 applies to the type of *firms* listed in *SUP* 15.1.3DR.

…

15.1.3B D …

15.1.3C R In addition to *firms*, the *rules* and *guidance* in *SUP* 15.18 also apply to:

(1) *payment service providers*;

(2) *UK RIEs*;

(3) *registered trade repositories*; and

(4) *registered credit rating agencies*.

15.1.3D R The *rules* and *guidance* in *SUP* 15.19 apply to:

(1) *firms* that are:

(a) *enhanced scope SMCR firms*;

(b) *banks*;

(c) *designated investment firms*;

(d) *building societies*;

(e) *Solvency II firms*; or

(f) *CASS large firms*;

(2) *UK RIEs*;

(3) *authorised electronic money institutions* and *authorised payment institutions*; and

(4) *consolidated tape providers*.

…

15.3 General notification requirements

…

Communication with the appropriate regulator in accordance with Principle 11

…

15.3.10 G …

15.3.10A R Any notification required under both *SUP* 15.3.8G(1)(e) and *SUP* 15.19 (Notification of material third party arrangement) should be made in accordance with *SUP* 15.19, which requires notification using the template specified in *SUP* 15 Annex 16R.

15.3.10B G The notification requirement under *SUP* 15.3.8G(1)(e) relates to a *firm's material outsourcing* arrangements. On the other hand, *SUP* 15.19 relates to the notification of *material third party arrangements* which include *material outsourcing* arrangements, although *SUP* 15.19 only applies to a specific group of *firms* (see *SUP* 15.19.1R). Consequently, some matters that need to be notified under *SUP* 15.3.8G(1)(e) may also have to be notified under *SUP* 15.19. In this case, there is no need to make the same notification twice but the *firm* concerned should make the notification in accordance with *SUP* 15.19.

…

Insert the following new sections, SUP 15.18 and SUP 15.19, after SUP 15.17 (Notification of regulated income by limited scope SMCR benchmark firm). The text is not underlined.

15.18 Notification of operational incident

Application

15.18.1 R This section applies to:

(1) a *firm*;

(2) a *payment service provider*;

(3) a *UK RIE*;

(4) a *registered trade repository*; and

(5) a *registered credit rating agency*.

15.18.2 R In this section, a reference to a *firm* includes:

(1) a *payment service provider*;

(2) a *UK RIE*;

(3) a *registered trade repository*; and

(4) a *registered credit rating agency*.

Purpose

15.18.3 G The purpose of this section is to set out the requirements for *firms* to notify the *FCA* of *operational incidents*, including the notification threshold and the process, timing and content of notification.

Initial report

15.18.4 R A *firm* must submit to the *FCA*, so far as it is aware, the information specified in the incident reporting data tables for the initial form in *SUP* 15 Annex 15R (referred to in this section as an 'initial report'), as soon as is practicable after the occurrence of an *operational incident* which:

(1) could cause or has caused intolerable levels of harm to *consumers* from which *consumers* cannot easily recover;

(2) could pose or has posed a risk to market stability, market integrity or confidence in the *UK financial system*; or

(3) could pose or has posed a risk to the safety and soundness of the *firm* and/or other market participants.

Intermediate report

15.18.5 R (1) A *firm* must, as soon as is practicable after any significant change in circumstances from that described in the initial report submitted under *SUP* 15.18.4R (including the incident being resolved), so far as it is aware, submit to the *FCA* the information specified in the incident reporting data tables for the intermediate form in *SUP* 15 Annex 15R (referred to in this section as an 'intermediate report').

(2) If there is any significant change in circumstances from that described in the last intermediate report submitted by the *firm* (either under (1) or in a subsequent intermediate report) (including the incident being resolved), the *firm* must, as soon as is practicable after such change, so far as it is aware, submit to the *FCA* another intermediate report.

Final report

15.18.6 R A *firm* must provide the *FCA* with the information specified in the incident reporting data tables for the final form in *SUP* 15 Annex 15R:

(1) within 30 *working days*; or

(2) where this is impracticable, as soon as is practicable but not exceeding 60 *working days*,

of the *operational incident* in *SUP* 15.18.4R being resolved.

Method of submitting the reports

15.18.7 R A *firm* must submit the reports required under this section to the *FCA* by completing the data fields online through the appropriate systems accessible from the *FCA's* website.

15.18.8 G Under this section, *firms* are required to notify the *FCA* only of an *operational incident* that has crystallised, as opposed to an incident that did not occur because of measures taken to prevent it from crystallising. Therefore, incidents that were averted do not need to be notified under this section. *Firms* should, however, consider notifying the *FCA* of such incidents under *SUP* 15.3.1R and *Principle* 11.

15.18.9 G When a *firm* experiences an *operational incident*, it should assess whether the incident has breached any of the notification thresholds set out in *SUP* 15.18.4R. The *firm* is required to notify the *FCA* of an *operational incident* under this section if it considers that one or more of the thresholds are breached. The *FCA* expects the *firm* to consider a range of factors when assessing whether any of the thresholds are breached, including but not limited to:

(1) the direct and indirect impact on the *firm's clients*, users of the *firm*'s services or the wider sector, including but not limited to its counterparties and other market participants;

(2) the *firm's* ability to provide adequate services;

(3) the reputation of the *firm* or the financial sector;

(4) the *firm's* ability to meet its legal and regulatory obligations; and

(5) the *firm's* ability to safeguard the availability, authenticity, integrity or confidentiality of information or data relating or belonging to a *client* of the *firm* or a user of the *firm*'s services.

General provisions

15.18.10 R *SUP* 15.6.1R to *SUP* 15.6.6G (Inaccurate, false or misleading information) also apply to *payment service providers*, *UK RIEs*, *registered trade repositories* and *registered credit rating agencies* that are required to make

notifications in accordance with this section as if a reference to *firm* in *SUP* 15.6.1R to *SUP* 15.6.6G were a reference to the relevant entity.

15.18.11 G Some matters that need to be notified by a *UK RIE* under this section may also have to be notified under *REC* 3.15 (Suspension of services and inability to operate facilities). A *UK RIE* should make separate notifications under both sections in this situation because the information that is required to be submitted under each section is different.

15.18.12 G *Payment service providers* should continue to comply with *SUP* 15.14.20D and *SUP* 15.14.21D in order to fulfil their obligations under regulation 99(1) of the *Payment Services Regulations*. However, *payment service providers* are required to submit notifications under this section, in addition to the notifications under *SUP* 15.14.20D and *SUP* 15.14.21D, only when one or more of the thresholds set out in *SUP* 15.18.4R are breached. Otherwise, *payment service providers* only need to submit notifications under *SUP* 15.14.20D and *SUP* 15.14.21D.

15.19 Notification of material third party arrangements

Application

15.19.1 R This section applies to:

(1) a *firm* that is:

(a) an *enhanced scope SMCR firm*;

(b) a *bank*;

(c) a *designated investment firm*;

(d) a *building society*;

(e) a *Solvency II firm*; or

(f) a *CASS large firm*;

(2) a *UK RIE*;

(3) an *authorised electronic money institution* or an *authorised payment institution*; and

(4) a *consolidated tape provider*.

15.19.2 R In this section, a reference to a *firm* includes:

(1) a *UK RIE*;

(2) an *authorised electronic money institution*;

(3) An *authorised payment institution*; and

(4) a *consolidated tape provider*.

15.19.3 R For the purposes of the definition of *material third party arrangement* and in this section, a reference to a *client*:

(1) in relation to a *UK RIE*, includes a *person* who is entitled, under an arrangement or agreement between them and that *UK RIE*, to use the *UK RIE's facilities*;

(2) in relation to a *consolidated tape provider*, includes a *person* who purchases a *consolidated tape for bonds* from:

(a) a *consolidated tape provider*; or

(b) a *data vendor*; and

(3) in relation to a *firm* carrying on the activity of *managing a UK UCITS* or *managing an AIF*, includes:

(a) a *unitholder*; and

(b) an investor in an *AIF*.

Purpose

15.19.4 G The purpose of this section is to set out the requirements for the *firms* specified in *SUP* 15.19.1R to notify the *FCA* of any new, or any significant changes to, *material third party arrangements*. This information, together with the *material third party arrangements* register information collected under *SUP* 16.33, will assist the *FCA* in understanding and overseeing *firms'* third party risks.

Notification requirement

15.19.5 R A *firm* must give the *FCA* notice when entering into, or significantly changing, a *material third party arrangement*.

15.19.6 R For the purposes of submitting the notice required in *SUP* 15.19.5R, the *firm* is not required to submit information on arrangements relating to:

(1) functions that are statutorily required to be performed by a service provider where the *FCA* already receives the related information (for example, through a statutory audit); or

(2) basic utilities (for example, electricity, gas and water), except telecommunication services and data storage services.

15.19.7 R A *firm* must submit the notice required in *SUP* 15.19.5R to the *FCA*:

(1) by using the template specified in *SUP* 15 Annex 16R; and

(2) online through the appropriate systems accessible from the *FCA*'s website.

15.19.8 G The *FCA* expects a *firm* to discuss relevant matters with it at an early stage and submit the notice required in *SUP* 15.19.5R before making any internal or external commitments.

15.19.9 G When assessing whether a *third party arrangement* is a *material third party arrangement*, the *firm* should consider the impact of the arrangement, with factors including but not limited to:

(1) the direct connection to the performance of *regulated activities*, the provision of *payment services* and the issuance of *electronic money*, *exempt activities* or *data reporting services*;

(2) the size and complexity of the business areas or functions supported by the *third party arrangement*;

(3) the potential impact of a disruption or failure in performance of the *third party arrangement* on:

(a) the *firm's* business continuity, operational resilience and operational risk;

(b) the *firm's* ability to comply with legal and regulatory requirements;

(c) the *firm's* ability to conduct appropriate audits of the relevant function, service or service provider;

(d) the *firm's* ability to identify, monitor and manage all risks;

(e) the *firm's* obligations under the *FCA Handbook*;

(f) the *firm's* obligations under the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity of the *firm* and its *clients*, including but not limited to the *General data protection regulation* and the Data Protection Act 2018; and

(g) the *firm's clients* or counterparties;

(4) the *firm's* ability to scale up the third party service; and

(5) the *firm's* ability to substitute the service provider or bring the outsourced service back in-house, including estimated costs, operational impact, risks, and timeframe of doing so in stressed and non-stressed scenarios.

Insert the following new annexes, SUP 15 Annex 15R and SUP 15 Annex 16R, after SUP 15 Annex 14R (Notification Procedures for Changes to the Management Body for Non-SMF Directors). The text is not underlined.

15 Annex 15R **Incident reporting data tables**

This annex sets out the data fields for the initial form, intermediate form and final form that are required to be completed under *SUP* 15.18.4R to *SUP* 15.18.6R. The data fields can be found through the following address:

[*Editor's note*: see Appendix 2 of this Consultation Paper]

15 Annex 16R **Material third party arrangement notification template**

The template can be found through the following address:

[*Editor's note*: see Appendix 3 of this Consultation Paper]

Amend the following text as shown.

16 **Reporting requirements**

16.1 **Application**

…

16.1.1F R …

16.1.1G R In addition to the type of *firms* listed in *SUP* 16.1.3R, the *rules* and *guidance* in *SUP* 16.33 also apply to:

(1) *UK RIEs*;

(2) *authorised electronic money institutions* or *authorised payment institutions*; and

(3) *consolidated tape providers*.

…

16.1.3 R Application of different sections of SUP 16 (excluding SUP 16.13, SUP 16.15, SUP 16.22 and SUP 16.26)

(1) Section(s)	(2) Categories of firm to which section applies	(3) Applicable rules and guidance

…			
SUP 16.32	…		…
SUP 16.33	A *firm* that is:		Entire section
	(1)	an *enhanced scope SMCR firm*;	
	(2)	a *bank*;	
	(3)	a *designated investment firm*;	
	(4)	a *building society*;	
	(5)	a *Solvency II firm*; or	
	(6)	a *CASS large firm*.	
…			

…

16.3 General provisions on reporting

…

Structure of the chapter

16.3.2 G This chapter has been split into the following sections, covering:

…

(26) *financial promotion approval* reporting (*SUP* 16.31); ~~and~~

(27) access to cash reporting (*SUP* 16.32)~~.~~; and

(28) *material third party arrangements* register (*SUP* 16.33).

…

Insert the following new section, SUP 16.33, after SUP 16.32 (Access to cash reporting). The text is not underlined.

16.33 Material third party arrangements register

Application

16.33.1 R This section applies to:

(1) a *firm* that is:

(a) an *enhanced scope SMCR firm*;

(b) a *bank*;

(c) a *designated investment firm*;

(d) a *building society*;

(e) a *Solvency II firm*; or

(f) a *CASS large firm*;

(2) a *UK RIE*;

(3) an *authorised electronic money institution* or an *authorised payment institution*; and

(4) a *consolidated tape provider*.

16.33.2 R In this section, a reference to a *firm* includes:

(1) a *UK RIE*;

(2) an *authorised electronic money institution*;

(3) an *authorised payment institution*; and

(4) a *consolidated tape provider*.

16.33.3 R For the purposes of the definition of *material third party arrangement*, a reference to a *client*:

(1) in relation to a *UK RIE*, includes a *person* who is entitled, under an arrangement or agreement between them and that *UK RIE*, to use the *UK RIE's facilities*;

(2) in relation to a *consolidated tape provider*, includes a *person* who purchases a *consolidated tape for bonds* from:

(a) a *consolidated tape provider*; or

(b) a *data vendor*; and

(3) in relation to a *firm* carrying on the activity of *managing a UK UCITS* or *managing an AIF*, includes:

(a) a *unitholder*; and

(b) an investor in an *AIF*.

Purpose

16.33.4 G The purpose of this section is to set out the requirements for the *firms* specified in *SUP* 16.33.1R to maintain a register for their *material third party arrangements* and to provide such information to the *FCA* in a standard format. This information, together with the *material third party arrangements* notification collected under *SUP* 15.19, will assist the *FCA* in understanding and overseeing *firms'* third party risks.

Requirement to maintain and submit a register

16.33.5 R A *firm* must:

(1) maintain a register of information relating to its *material third party arrangements*; and

(2) submit the register of *material third party arrangements* annually to the *FCA*.

16.33.6 R For the purposes of submitting the register required in *SUP* 16.33.5R(2), the *firm* is not required to submit information on arrangements relating to:

(1) functions that are statutorily required to be performed by a service provider where the *FCA* already receives the related information (for example, through a statutory audit); or

(2) basic utilities (for example, electricity, gas and water), except telecommunication services and data storage services.

16.33.7 R The *firm* must submit the register of *material third party arrangements* specified in *SUP* 16.33.5R(2) to the *FCA*:

(1) using the template specified in *SUP* 16 Annex 59R; and

(2) online through the appropriate systems accessible from the *FCA*'s website.

16.33.8 G When assessing whether a *third party arrangement* is a *material third party arrangement*, the *firm* should consider the guidance set out in *SUP* 15.19.9G.

Insert the following new annex, SUP 16 Annex 59R, after SUP 16 Annex 58R (Guidance notes for the Pensions Dashboard Service Firms – Half-Yearly Prudential Report). The text is not underlined.

16 Annex 59R **Material third party arrangements register template**

The template can be found through the following address:

[*Editor's note*: see Appendix 3 of this Consultation Paper]

Amend the following text as shown.

Sch 1 Record keeping requirements

…

Sch 1.2 G

Handbook reference	Subject of record	Contents of record	When record must be made	Retention period
…				
SUP 16.8.23R [FCA] [PRA]	…	…	…	…
SUP 16.33.5R(1)	*Material third party arrangements*	Register of information relating to *material third party arrangements*	Not specified	Not specified

Appendix 2

Data tables: Incident Reporting

Operational incident reporting – https://www.fca.org.uk/publication/forms/incident-reporting-fields-document.xlsx

Appendix 3

Data tables: Third party reporting

Third party reporting – https://www.fca.org.uk/publication/forms/mtp-reporting-template.xlsx

Pub ref: 2-008237

12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk