

Operational Resilience: Operational incident and Third Party Reporting



FCA & PRA Consultation Paper

UK Finance response

Contents

Introduction	4
Recommendations	6
General Recommendations.....	6
Operational Incident Reporting Recommendations	6
Cost-Benefit Analysis Recommendations.....	6
Third-Party Risk Management Recommendations	7
Reporting Templates & Submission Recommendations	7
Regulatory Coordination Recommendations	7
Responses to consultation question set	8
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?	8
Question 2: Do you agree with the proposed definition of an operational incident?	11
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?	13
Question 4: Do you agree with the proposed approach to standardise the formats of incident reporting?.....	16
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?	18
Question 6: Do you agree with the proposed definition of third party arrangements?	20

Question 7: Do you agree with the proposed definition of material third party arrangements?.....	21
Question 8: Do you have any comments on our proposed notification requirements including the impact on the number of arrangements that will be reported?	23
Question 9: Do you think the mechanism to submit and update the structured register of firms’ material third party arrangements is proportionate?	25
PSD2 Commentary	28
Summary	30

Introduction

UK Finance welcomes the opportunity to respond to the PRA's and FCA's consultation papers CP24/28 and CP17/24, which seek to refine the frameworks governing operational incident reporting and third-party risk management.

As the voice of the UK financial sector, representing approximately 300 firms, we recognise the importance of ensuring regulatory effectiveness, clarity, and proportionality in these areas.

The proposals set out in the consultation introduce significant changes to the incident reporting regime, including new definitions of operational incidents, revised thresholds for reporting, and enhanced third-party oversight requirements. While we acknowledge the regulators' objectives, particularly in enhancing resilience, supervisory oversight, and cross-sector consistency, UK Finance contends that existing regimes (such as PSD2) need to be rationalised or removed before new rules enter into force.

This response sets out several key concerns that must be addressed to ensure that the proposed changes are both practical, effective and limit undue burden on the sector.

A key issue in the overall approach of the proposals being put forward is the utilisation of a reporting regime for the purposes of data collection or improving resilience of firms. The approach further seeks to expand the operational resilience regime across FCA-regulated firms that are not in-scope of the resilience rules. It is UK Finance's view that this should not be the intent of reporting but the basis of separate rules, such as the previously mentioned operational resilience regime.

Our Members highlight that both the PRA and FCA have extensive rules that allow for data collection and can request information via a variety of sources. Should the PRA and FCA wish to collect data relating to incidents, members encourage this is undertaken via the existing methods and channels and that embedding data collection within incident management runs counter to the stated objectives and the intended function of incident management within financial institutions.

UK Finance note substantial underestimations in the consultation's cost-benefit analysis (CBA). The projected implementation costs fail to capture the true financial burden on firms, particularly those subject to multiple UK and international reporting regimes. Further, regulatory duplication remains a serious concern to our members, with proposals adding complexity and nonessential operational activity rather than streamlining existing requirements or aiding the regulator's objectives.

The proposed definitions of operational incidents and reporting thresholds also introduce ambiguity and could lead to excessive reporting obligations. It is our view that concepts such as "potential impacts," "operational contagion," and "reputational harm" expand the reporting net too widely and lack alignment with existing operational resilience frameworks. UK Finance strongly advocates for a more pragmatic and proportionate approach,

ensuring that incident management remains focused on remediation rather than a compliance activity.

UK Finance are keenly aware of the resource implications for different sized organisations when considering the operationalisation of these proposals. We contend that these demands could prove prohibitive for small to medium-sized firms, where resources might be better allocated to incident prevention rather than detailed documentation. The complexity is further exacerbated by the FCA's intention to apply the incident reporting regimes to firms who have not implemented the operational resilience rules, where subjective terminology will be less understood.

In relation to third-party risk management, we welcome the focus on material relationships but urge regulators to ensure consistency between the PRA's and FCA's frameworks. The expanded definitions of third parties, particularly the inclusion of non-outsourcing arrangements, may impose disproportionate burdens on firms and must be carefully refined.

Finally, if this was to be implemented, the proposed reporting templates and processes require considerable refinement. The current approach risks overburdening firms with excessive data collection requirements, misaligned reporting structures between the PRA and FCA, and operational challenges in submitting large-scale data. Regulatory coordination and simplification in this area are paramount to ensuring efficiency and effectiveness.

While at the date of submission the UK Government is yet to publish its "*Financial Services Growth and Competitiveness Strategy*" (expected in April 2025), the Chancellor has clearly signalled in a recent Mansion House speech¹ that [financial sector] regulation needs to be recalibrated as the authorities have been "*regulating for risk but not regulating for growth*". The requirements proposed could be viewed as running contrary to the pledge to '*make regulation work much better for our economy*' given the issues we explore throughout the body of this response.

In the sections that follow, UK Finance provides detailed responses to the consultation's questions, highlighting where adjustments are necessary to achieve a balanced and practical regulatory approach.

¹ <https://www.freshfields.com/en-gb/our-thinking/knowledge/briefing/2024/11/the-2024-mansion-house-speech-and-the-future-of-uk-financial-services/>

Recommendations

General Recommendations

- The cost-benefit analysis (CBA) needs revision to reflect the true cost of compliance, particularly for large and internationally regulated firms.
- Regulatory alignment between the FCA and PRA is essential to avoid inefficiencies, duplication, and unnecessary complexity.
- Existing regimes (such as PSD2) need to be rationalised or removed before new rules enter into force.
- A proportionate approach should be taken in defining incident reporting thresholds and third-party reporting requirements, ensuring firms are not overburdened.

Operational Incident Reporting Recommendations

- Revise the definition of an operational incident to better align with the UK's existing operational resilience framework, ensuring clarity and consistency.
- Embed recognition of firm's internal classification severity levels in the thresholds to propose a more outcomes-focused regime where firms are able to match their severity levels with the regulator's mandates.
- Exclude "potential impacts" from the definition to prevent firms from having to report near misses, which would add unnecessary reporting volume.
- Remove the requirement to report on operational contagion and indirect impacts, as these are subjective and difficult to measure.
- Provide greater flexibility on incident reporting deadlines, particularly the 30-working-day deadline for final reports, allowing firms more time for thorough investigations.
- Clarify the distinction between "resolved" and "recovered" incidents, ensuring firms have clear reporting expectations.
- Remove the requirement for legal/regulatory non-compliance as an incident threshold, as this would force firms to speculate on potential regulatory breaches.
- Reassess the requirement for reporting reputational impact, as this could lead to overreporting due to media speculation rather than actual harm.

Cost-Benefit Analysis (CBA) Recommendations

- Re-evaluate implementation cost assumptions, which UK Finance believes are significantly underestimated.
- Incorporate the cost of regulatory duplication into the CBA, particularly for firms that must comply with PSD2 reporting alongside the new regime and those that are dual regulated.
- Acknowledge the resource impact on firms, especially those required to mobilise dedicated teams, develop new policies, and provide continuous training.

- Consider the additional Requests for Information (RFIs) that regulators routinely issue after incident reports, adding further compliance burdens.

Third-Party Risk Management Recommendations

- Narrow the scope of third-party reporting to material outsourcing arrangements, ensuring that firms do not need to report non-critical supplier relationships.
- Ensure consistency in definitions between the FCA and PRA for third-party arrangements, reducing uncertainty and implementation challenges.
- Clarify how intra-group arrangements should be treated, particularly where subsidiaries operate under different regulatory regimes.
- Reassess expectations for mapping operational chain risks, as firms may struggle to track Nth-party providers deep in their supply chains.
- Adopt a risk-based approach where firms determine material third-party relationships based on internal classification criteria.

Reporting Templates & Submission Recommendations

- Ensure a single, unified reporting template between the FCA and PRA to streamline submissions and reduce operational inefficiencies.
- Remove unnecessary data fields from the templates that do not contribute meaningfully to supervisory oversight. (specific examples provided below)
- Provide firms with the flexibility to mark certain fields as “not applicable” rather than requiring excessive data collection.
- Address discrepancies between PRA and FCA templates, including the number of data fields, terminology differences, and structural inconsistencies.
- Allow firms to bulk-upload data with minimal manual input, ensuring efficient submission processes.
- Clarify requirements for third-party notification timelines, particularly around the meaning of “internal commitments” before formal agreements.

Regulatory Coordination Recommendations

- Remove the requirement for PSD2 incident reporting, as the new operational incident framework should replace this outdated regime.
- Improve coordination with international regulatory standards, ensuring UK financial institutions are not placed at a competitive disadvantage.
- Engage further with industry stakeholders before finalising the proposals to ensure practical implementation.

Responses to consultation question set

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?

1. UK Finance has concerns about the assumptions and calculations underlying the cost-benefit analysis (CBA) presented in the consultation paper. The estimated implementation costs appear to be significantly underestimated, particularly for larger organisations.

1.1. UK Finance acknowledge that while members were indeed directly engaged by the authorities for empirical data to support the CBA, there was likely to have been a communications disconnect in this process. It is almost certain that this led to a failure of firms to comprehend the full implications of the questions and thus provide incomplete data.

2. UK Finance specifically challenges the annual estimated costs put forward in the consultation (£40,000-£100,000) as we believe these figures could increase substantially.

2.1. One Member states that DORA implementation costs reported till now highlight how similar reporting regimes have resulted in significant cost to some firms:

- 2.1.1.1. GPB2.3m for “Change the Bank” CtB (Q4/2024 - Q4-2025)
- 2.1.1.2. GPB3.8m for “Run the Bank” RtB (Q4/2024 - Q4-2025)

3. The implementation burden encompasses several key areas that UK Finance assess have not been adequately accounted for. Organisations would need to mobilise dedicated project teams, implement new systems for data recording and reporting, conduct relevant staff training activities, and develop or adapt existing policies, procedures, and controls. Furthermore, ongoing compliance would require dedicated incident managers and second-line monitoring resources, with these human resource requirements likely to grow as firms expand. All incident reports sent to regulators require rounds of approval and, often, confirmation by a relevant Senior Manager (SMF24). The additional resource and capacity competes with incident management and other productive activities for time and attention, which all place a downstream cost on the functioning of the financial institution.

4. A significant industry concern centres on the continued effect of PSD2 incident reporting in UK legislation and the FCA Handbook. UK Finance has noted some concern amongst members about the FCA's inability to amend their rulebook and establish a single reporting regime (in a similar fashion to the EU's Digital Operational Resilience Act -

DORA). This regulatory duplication is viewed by our members as creating an unnecessary competitive disadvantage that should be reflected negatively in the cost-benefit analysis.

5. UK Finance would like to express that both formal and informal incident reporting regimes (alongside dual regulated firms being subject to two criteria and some international firms being subject to approximately 150 international regimes) is not adequately noted in the proposals set out in this consultation. Additionally, the requirement for multiple intermediate reports can be seen as an excessive burden when compared to other international regimes. Reports required under PSD2 alongside informal regimes under PRA Principle 11 and Fundamental Rule 7 should be acknowledged. The CBA should include a potential situation whereby a firm is subject to multiple UK regimes. A PSD2 initial report is due within 4 hours, further reporting is due under the current regime (across two criteria) and all require multiple iterations of intermediate reports (the FCA's criteria for intermediate being when 'additional information' is found).

5.1. As a practical example of how this burden can manifest, one member firm had a PSD2 report with fifteen intermediate reports required. Under the proposed UK regime, in a similar scenario the firm would have to submit thirty reports with competing deadlines occurring across PSD2, UK IR, and informal updates to UK supervisors. UK Finance do not believe that this level of compliance activity is proportionate to the risk management benefits or reflective of a regime that is pro-business. This cost and diversion from incident management should be reflected within the CBA.

6. Members who are dual regulated firms note that they face two competing criteria by the PRA and FCA, requiring separate internal governance, and can have informal agreements to inform supervisors regarding incidents. The number of regimes, therefore, across two regulatory institutions in the UK, can be accurately viewed as five. Members would welcome clarification from the authorities that with the implementation of any new regime, supervisory teams will be instructed to reevaluate and cancel any reporting agreements in place with firms save for those with a clear justification.

7. As an international financial centre, the CBA, in addition, does not reflect the cost of firms being subject to multiple incident reporting regimes across multiple jurisdictions. Incident management is often centred within individual centres of excellence to ensure effective remediation. A comparison of the UK incident reporting approach and competitiveness vis-à-vis other international financial centres should be included within the CBA. The practice of argumentation of why the UK is following a particular approach, as is often used within prudential rulemaking, should be followed with resilience-related regulation.

8. The CBAs of both the PRA and FCA do not acknowledge the additional Requests for Information (RFIs) that all firms face when reporting incidents to their supervisors. RFIs often require expedited/ real-time responses with granular information relating to the individual incident(s). This often places significant extra burden on incident management teams to reflect the RFI under direct supervisory pressure. While firms appreciate the

comment regarding increased clarity, members are circumspect in practice due to experiencing RFIs across both respective regulators. Additional expectations of reporting figures will result in further increased expectations of RFIs, which adds to the administrative resource being required to reflect the new regimes. Roundtables with policymakers have resulted in further uncertainty for firms regarding the interaction of the regime with their dedicated supervisory teams.

9. The timing of these proposed changes has also drawn critique within the broader regulatory context. UK Finance member engagement has pointed out that the financial services sector is simultaneously grappling with Consumer Duty changes, operational resilience requirements, and preparing for Rulebook modifications. This cumulative regulatory burden, with competing reporting regimes, is seen as particularly challenging at a time when the government is advocating for reduced regulation to support growth.

10. UK Finance challenges the fundamental assumptions about benefits. The assertion that increased incident reporting would lead to fewer incidents is questioned. In addition, members reject that reporting regimes should be utilised to encourage a change in firm behaviour. In order to improve a firm's ability to respond to incidents, both regulators have introduced operational resilience regimes and supervise firms directly. Given that regulators already hold powers to improve the effectiveness of incident management, such as Section 166, members reject that the improvement of incident management should be the objective of the proposed regime.

11. In regard to consistency of data and the capturing of trend data, UK Finance asserts that reporting with short deadlines should not be the method for this type of data collection. Individual supervisory teams can already be tasked with examining incident management and reporting practices, internal thresholds and the collection of historic incidents. Given this, we contend that the lack of data consistency is unlikely to be a substantive problem to the authorities. The root cause of the incident, whether it be malicious cyber, tech change etc. would be readily apparent from any report. Furthermore, it should be apparent that facts and figures on impact are not necessary for mitigating risk, only for quantifying and justifying interventions.

12. Regarding third party considerations, UK Finance would like to highlight potential additional costs that could be passed through from third parties required to provide outage reporting.

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

13. UK Finance highlights that there are concerns about the breadth, clarity, and practical implementation of the proposed operational incident definition.

14. The subjectivity regarding the definitions, and the assessment criteria, is compounded by the PRA and the FCA stating that the regime does not align with the existing operational resilience regime and should be applied more widely. This is despite both assessment criteria aligning fully with the definitions of intolerable harm included in both operational resilience regimes. Members strongly reject that the regimes should not be aligned, and that further effort should be made to ensure full alignment. UK Finance's members have comprehensive resilience frameworks in place that align internal incident classification with the operational resilience regimes in the UK. Creating alternative definitions and criteria for intolerable harm creates too much complexity and risks confusing existing regulation and firms' compliance.

15. UK Finance acknowledges that the PRA and FCA supervisors could be concerned that a fully aligned incident reporting regime with the operational resilience regime and a firm's internal classification could result in incidents being missed from reporting. Members reject this could be the case if the bedrock of Principle 11 and Fundamental Rule 7 informal reporting was maintained. In order for firms to comply with the proposed regime, they would adapt their existing internal classifications and add their subjective interpretation of the proposed criteria. It is unclear why a more complicated regime, across multiple differing criteria and examples, is necessary and it does not reflect the reality of how incident management occurs within firms. UK Finance would appreciate a discussion with supervisors or policymakers concerning why a more complicated regime is required and where the subjectivity would remain a risk.

16. The inclusion of "potential" impacts has drawn particular scrutiny with members - UK Finance seeks confirmation from the regulators that they do not seek to capture near-misses within reporting. UK Finance agree that this could unnecessarily encompass additional reporting for impacts that fail to materialise. We suggest that "potential impacts" should either be excluded entirely or treated differently from actual impacts. There is an additional risk that firms report on the basis of unrealised information directly to supervisors. This is a risk to firms and would remove the regime from the practical operations of their incident management teams. Risk regarding potential incidents would be maintained by the continued application of Principle 11 and Fundamental Rule 7.

17. Equally, the PRA and FCA include 'operational contagion' and 'indirect impacts'. During an incident, with firms primarily focusing on resolution and the impacts of an incident to their ability to deliver their own IBS, UK Finance contend that any requirement to accurately assess wider implications may be placing undue burden and drawing resources away from remediation activities. Analysing 'potential' impacts of 'contagion' or 'indirect' impacts is disproportionate and misdirects incident management teams from

remediation. It is also outside the capabilities of any of the members we have spoken to and its practicability should be regarded with scepticism.

18. An important new concept introduced in the definition is "operational contagion." UK Finance note that this concept, while referenced in various regulatory contexts, including the FMI Fundamental Rules and Critical Third Party regime, has not been subject to consultation or industry feedback. Operational contagion should be seen first and foremost as a planning tool for resilience, not a practical decision-making criteria for crisis situations. We advocate for dedicated consultation and industry engagement before embedding this concept in regulatory expectations. UK Finance contend that the incident management process is an unsuitable process to embed concepts of "operational contagion" and should be considered within operational resilience regimes before proliferation in other rules.

19. UK Finance has concerns about alignment and duplication with existing reporting requirements. Members point out that they already undertake considerable operational incident reporting under frameworks such as PSD2 and informal Principle 11 and Fundamental Rule 7, suggesting this new definition might create redundant reporting obligations. This highlights significant anti-competitiveness and an over-production of regulatory rulemaking. Members support the removal of PSD2 reporting, which has a materially different approach to the regimes proposed by the PRA and FCA.

20. Given the breadth of the operational incident definition, Members suggest that the "or" before the second clause of the definition should be changed to "and". This would help limit any requirement to understand impacts to data held externally which might be beyond the visibility of financial services firms and already captured by the Critical Third Parties regime.

21. UK Finance suggests that individual firms need flexibility to build their own metrics proportionate to their size and business complexity. Members therefore believe that greater recognition should be placed on the use of their internal classification criteria to determine whether reports are required. These are often predicated on the availability of services, Important Business Services being affected, and customer-impact amongst other criteria depending on the Line of Business. The PRA and FCA could provide non-binding guidance on what firms should consider within their classification alongside the operational resilience regime as the basis of incident reporting.

22. The case studies provided in CP24/28, while appreciated, are seen as insufficient given the breadth of scenarios firms might encounter. Case study 5, in particular, is cited as introducing potentially problematic concepts like "adequate services" that could extend beyond Important Business Services. While firms acknowledge why the case studies and examples are used, members recommend these are simplified (e.g. a destructive cyber attack) and focus on a firm's internal classification instead of hypothesized impacts which serve to add greater confusion due to the extent of firms regulated across the PRA and FCA.

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?

23. The industry supports the recognition of internal firm incident classifications in the PRA's regime and believes this should be extended to the FCA. UK Finance supports internal classifications being introduced as a secondary threshold alongside the regulatory mandates of the FCA and PRA. Effective cybersecurity practice for incident management is to create firm-wide internal classifications for incident severity as this allows for resource to be allocated appropriately, escalations to occur consistently, and be a basis for crisis management activity across the firm. Firms, in order to comply, will choose a severity level to map to the regulators' mandates and will triage this segment of incidents and above. Allowing firms to choose a severity level that maps to the regulators' mandates will achieve a simplistic and outcomes-focused regime and will remove the necessity for unnecessary triaging before the initial reporting stage. All assessment criteria should be considered guidance from the regulators concerning what severity level a firm should consider.

24. A fundamental issue emerges around the breadth and subjectivity of the thresholds. UK Finance highlights that including incidents that 'could cause' harm sets an extremely low reporting threshold that could lead to overreporting. Members note that this could encompass incidents that do not lead to the materialisation of significant harm, thereby complicating assessment processes. Subjective interpretation of 'could cause' harm should not be embedded within incident management as this detracts from management and remediation. Frequently, in the early stages of an incident, there is a great deal of information scarcity, which is only magnified by requirements to speculate on potential impacts. Firms may well feel the need to apply significant conservatism and report any incident for which they cannot definitively conclude (and evidence) there is no possibility of it meeting the thresholds, which is likely to be the majority of incidents.

25. There is often subjectivity regarding the direct impacts of incidents within firms due to how firms collect data depending on the particular service or IT infrastructure. To assess indirect impacts would require significant data and insight as to the operational, commercial and financial circumstances of firms' clients, customers and counterparties, far beyond what they can (and should) have visibility of. Any assessments of indirect impact are likely to prove extremely inaccurate and of little value to the regulators, while generating significant cost to firms, and distracting effort from the management of incidents during a critical period. While we understand that the regulators wish to use this information to garner greater insights as to firms' interconnectedness and to identify where impacted firms are not themselves submitting incident reports, it is the view of Members that the likely low level of reliability of this data, the detriment to incident management, and the cost associated with it, are not justified by these benefits.

26. UK Finance seeks clarity on the FCA's assessment factor regarding the firm's ability to provide adequate services doesn't consider the materiality of the service being disrupted. Many firms will have many services which can be significantly disrupted with minimal impact on customers or clients, let alone posing a risk to safety and soundness, UK financial stability, or intolerable levels of consumer harm. The FCA gives an example of "the firm being unable to meet its obligations to its clients or counterparties". This does not consider the degree of harm, or the criticality of such obligations, and so sets a very low bar for meeting the threshold. Another example, of "the firm being unable to avoid disruption causing harm to clients and counterparties", also fails to consider the materiality of harm caused, effectively setting the threshold to any harm at all. This is difficult to reconcile with the Thresholds of Financial Stability, Safety and Soundness or intolerable levels of consumer harm. In some circumstances it could be interpreted as seeking to set the tolerable level of consumer harm as zero, contrary to the approach taken in the Operational Resilience rules.

27. UK Finance acknowledges the concept of consumer harm as a threshold in relation to the FCA's respective mandate, however Members recommend that the FCA considers an alternative means to define consumer harm, based on a firm's internal classification and a continued recognition of internal severity assessments and Fundamental Rule 7 as a basis for interpretation.

28. The relationship between consumer harm and sector impact requires careful consideration. Members have expressed that there appears to be an inconsistency in how the respective thresholds treat these different groups. The consultation paper alternates between referring to "harm" and "intolerable harm" creating further potential confusion for firms in the operationalisation of these proposals.

29. Legal and regulatory non-compliance as an incident threshold has drawn particular doubts. UK Finance expresses serious concern about this requirement, noting that it could force reporting entities to speculate about potential legal exposure or regulatory breaches. Members point out that European lawmakers removed similar data fields from the Regulatory Technical Standards for major incident reporting under DORA, suggesting this precedent should be considered. This is notably under consideration by the FSB where UK Finance have responded against the inclusion of this criteria.

30. The reputational impact criteria have also been questioned. UK Finance highlights how threat actors are already weaponizing reputational requirements within incident reporting, creating fabricated incidents with media outreach to provoke market responses. Members recommend limiting reputational reporting to cases where firms have been unable to provide adequate services, rather than including more minor incidents that might appear in social media or local news. UK Finance requests that the regulators demonstrate a clear correlation between news coverage and losses of customers and / or business, while accounting for other related variables, before including such a measure.

31. The case studies provided in the consultation paper have received mixed feedback. While intended to clarify expectations, some members note significant discrepancies in the criticality of incidents described, pointing to the contrast between a complete digital bank IT infrastructure outage and a website being temporarily offline.
32. The concept of proportionality emerges as a recurring theme, particularly regarding data and information security incidents. UK Finance question whether small-scale incidents, such as unauthorised disclosure affecting a single individual, warrant regulatory reporting if no intolerable harm is identified. We suggest incorporating clearer proportionality principles into the reporting framework.
33. The relationship between Business Continuity Plans (BCPs) and reporting requirements needs clarification. The consultation fails to recognise the enormous investment that has been made under the operational resilience framework to put in place measures to avoid intolerable harm emerging when incidents take place. The proposals in this framework, in particular the framing around incidents which 'could cause' harm, fail to recognise the benefit and resilience that those measures offer in avoiding or minimising harm. Members specifically ask whether incidents (that are subsequently mitigated through BCPs or substitution before they reach the respective threshold of harm) still require reporting, highlighting a gap in the current guidance.

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

34. A central concern emerging from Members, focuses on the potential creation of parallel reporting regimes for PRA and FCA regulated firms. UK Finance highlights that while all incident reports will be submitted through the same FCA portal and received by both regulators, there remains ambiguity about how firms should handle incidents that meet both PRA and FCA criteria. For dual-regulated financial institutions, this creates uncertainty about regulatory responses to incident reports and raises questions about potential duplication of effort. This would be exacerbated by the greater pressure placed on firms through RFIs by their respective supervisors.

35. Timeline considerations are a significant area of concern amongst UK Finance members. Several members indicate that the proposed 30-working-day deadline for final incident reports may be insufficient, particularly for incidents involving third parties where firms depend on external root cause analyses. With this in mind, UK Finance advocates for firms' reporting requirements to be *"as soon as practicable; but not exceeding 60 days with the possibility of exemptions and extensions if needed"*. We also query the distinction between *"resolved"* and *"recovered"* in paragraph 3.35, highlighting the need for precise terminology in reporting requirements.

36. The relationship with existing reporting frameworks, particularly PSD2 Incident Reporting, requires amendment and reconsideration by the PRA and FCA. UK Finance explicitly note that according to FCA's CP clause 3.53, these new requirements do not replace PSD2 obligations, potentially creating burdensome parallel reporting requirements.

37. UK Finance therefore strongly support the repeal of PSD2 incident reporting. This can be achieved via a statutory instrument repealing 'The Payment Services Regulations 2017, SI 2017/752, Part 7, Regulation 99' subject to the implementation of the proposed rules. Additionally, the FCA has the capability to provide firms with waivers or modifications which allow non-compliance with specific rules. Members therefore support a statutory instrument, that could be introduced via a Financial Services Bill, being put into effect before the implementation deadline or a waiver to PSD2 reporting for all payment service providers operating in the UK. This would result in the single reporting approach in the UK.

38. UK Finance acknowledge the potential benefits of standardised reporting but emphasise the need for balance between information depth and response speed. There are calls for understanding how this information would be collected, assessed, and utilised for improving industry resilience.

39. Members are concerned that the PRA and FCA could be utilising a reporting regime for the purposes of data collection or improving resilience of firms. This should not be the intent of reporting but the basis of separate rules, such as the existing operational resilience regime. The PRA and FCA both already hold extensive powers that allow for data collection and should the PRA and FCA wish to collect data relating to incidents,

Members encourage this is undertaken via these existing routes. UK Finance contend that embedding collection within incident management runs counter to the stated objectives and the intended function of incident management within financial institutions.

40. The resource implications for different-sized organisations emerge as a significant concern. UK Finance notes that these demands could prove prohibitive for small to medium-sized firms, where resources might be better allocated to incident prevention rather than detailed documentation. This serves to better encourage the recognition of internal classification criteria in the regime instead of complicating the regime with case studies, competing assessment criteria and indirect impact/ operational contagion. UK Finance further reiterates their view that a firm should be able to match an internal severity level to the regulator's mandates and this should be embedded in the thresholds for reporting. This would aid small to medium-sized firms, who would not have been in-scope of the operational resilience regime nor have the sophistication necessary to analyse incidents to the extent required in both the FCA's and PRA's regimes. Larger firms would be aided as they will have mature incident management capabilities and would face a substantially higher proportion of RFIs from supervisors during the incident occurrence.

41. UK Finance suggests that while the industry generally supports moves toward standardised reporting (albeit not when PSD2 remains in effect), the current proposals require significant refinement to address practical implementation challenges, reduce duplication, and ensure reporting requirements remain proportionate to both firm size and incident severity.

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?

42. UK Finance agree with the principle of proportionate notification, though significant concerns have emerged amongst Members about the practical implementation and resource implications. Members have noted the potential for issues to arise given the volume and complexity of the reporting requirements.

43. A fundamental challenge emerges regarding the concept of financial and operational contagion. One Member highlights the significant limitations firms face in assessing third party impacts, particularly regarding financial capabilities during operational incidents. UK finance notes that financial institutions have limited ability to evaluate how incidents might affect third parties' liquidity positions, access to funding sources, price discovery capabilities, or ability to make margin payments. This raises important questions about the practicality and accuracy of such reporting requirements and may raise legal issues in the case of the dissemination of information that subsequently turns out to be false or inaccurate.

44. UK Finance's members have concerns regarding the criteria being proposed for "significant change" for intermediate reports. This, notably for the FCA, appears to encompass any 'additional information' in relation to the individual incident. This reflects the lowest threshold for any report and would result in overreporting. This is notably a significant burden with PSD2 reporting, due to PSD2 reports requiring another intermediate report if information remains estimated. Information regarding incidents are often estimations and gradually increase through incident management. The criteria provided by the PRA and FCA for the intermediate report should be more proportional and reflect the realities of how incidents are managed.

45. UK Finance recognises that the PRA and FCA have considered reducing the regulatory burden by not enforcing intermediate reports. Members appreciate this intent and propose that alternative measures for "significant change" could be based on the severity of the incident increasing according to the internal classification of the firm. This could further recognise the role of Principle 11 or Fundamental Rule 7 in terms of information that would be important for the regulator to know during the process of incident remediation. UK Finance encourages that the FCA adds a proportionality statement into its "significant change" description to provide more clarity to firms and remove the potential for overreporting.

46. UK Finance advocates for a consistent template structure where fields can be marked as "not applicable" rather than being entirely omitted. Careful consideration should

be given to avoid information gaps. This approach would help ensure comprehensive data collection while maintaining flexibility for different incident types.

47. For smaller firms, the volume of required data fields presents particular challenges. Some members note that extensive reporting requirements could divert resources from actually addressing the incident, especially during initial reporting phases. UK Finance suggest a proportional approach by pushing non-essential data collection requirements to the final reports, allowing firms to prioritise incident management in the crucial early stages.

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

48. The proposed definition for third party arrangements reflects an expanded scope to include both outsourcing and non-outsourcing arrangements. It is understood that this is necessary to address the risks posed to firms and the stability of the UK financial system, and to meet the regulators' stated objectives. As this expanded definition would require firms to capture a significantly broader population of third-parties as part of the proposed reporting and notification requirements, the regulators' focus on material third party arrangements is welcomed. To avoid a potentially disproportionate and substantial reporting burden, we have proposed some amendments to the definition of material third party arrangements below. We also suggest the definition of third party arrangements could be further refined to products and services provided "on a recurrent or ongoing basis" in line with the FSB Toolkit and DORA.

49. Whilst UK Finance understands that some divergence in approaches between the PRA and FCA may be necessary to give effect to their respective mandates and statutory objectives, we believe there are opportunities to further align these approaches throughout the proposed framework. Specifically, we welcome consistency in terminology across frameworks and definitions, noting that the PRA/BoE refers to "person," whilst the FCA uses "service provider" in their respective definitions of third party arrangement. Such variation in terminology could create unnecessary complexity in implementation and interpretation. The suggestion for aligned language across regulators reflects a broader desire for regulatory coherence.

50. The definition makes reference to "An arrangement of any form between a firm and service provider". It would be helpful if the regulators could elaborate on this to make explicit that the focus is on instances in which a service provider provides a service to the firm, and not a business referral.

51. A key area requiring clarification centres on intragroup arrangements, particularly regarding the definition as '*provided by a person within the same group as the firm.*' UK Finance advocates for consistent terminology in regards to intragroup arrangements again, substituting 'person' with 'entity'.

52. UK Finance recommends where a service is 'provided directly or by a sub-contractor' that the definition is amended to 'provided directly or supported by a sub-contractor'.

53. UK Finance would like the PRA to clarify if their intention is to expand the Third Party reporting scope to include non-Vendor arrangements (i.e. FMI, cheque clearing houses). Furthermore, we request clarity on expected submission timeline/go-live date with suggestion on advance notice provided before the updated template goes live, especially where major changes are expected.

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

54. UK Finance strongly supports limiting the register and notification requirements to material third parties. This targeted approach supports effective and risk-based reporting practices, helping to ensure proportionate reporting and oversight practices. However, we note that the use of “*pose a risk to*” in the definition of material third party arrangements is inherently broad. It risks capturing arrangements that may have a merely theoretical potential for harm and diverge from the regulators’ intended objective to capture those arrangements that could have a tangible impact. We suggest the regulators replace “*pose a risk to*” with “*materially impair*” to ensure an appropriate emphasis on actual significant impacts and minimise the risk of overreporting.

55. Whilst a degree of divergence in the definition of material third party arrangements may be necessary to reflect supervisory objectives, we do not see the basis for divergence in the materiality assessment criteria and suggest that these are aligned between the PRA’s and FCA’s frameworks. This alignment would help reduce complexity in implementation and interpretation across different regulatory frameworks.

56. The intersection with materiality assessment criteria, particularly as outlined in SS2/21, needs clarification. UK Finance highlights new expectations regarding intragroup arrangements, specifically noting the clause that states, ‘PRA would not generally expect the following arrangements to be classified as material intragroup arrangements which do not involve an external third party provider.’ The FCA does not exclude intragroup arrangements from being deemed material, and we would encourage the FCA to adopt the PRA’s stance. If the PRA does not deem intragroup arrangements as material unless they involve an external third party provider, they will not need to be included in the third-party arrangement register submission, nor will they be notifiable under the regime outlined in the consultation. This will create a dual reporting regime in the UK where firms must include all intragroup arrangements in registers and notifications to the FCA but not the PRA. If the intention is to have a single register, submitted on a single platform for both the PRA and FCA, the PRA and FCA should align on the materiality of intragroup arrangements.

57. We suggest that receiving tens of thousands of rows “ranked 0” due to intragroup arrangement data both increases the burden of reporting for firms and negates the use and potential value of a ranking system. This could be avoided because all of a firm’s external arrangements will be reported at rank 1 with the recipient (of subcontracting) entity identified (in the case of intragroup, the service company).

58. Proportionality emerges as a key consideration, with UK Finance seeking more detailed information about what might fall outside the scope of these requirements, noting that certain services like market data provisions are excluded under EBA guidelines.

59. While the PRA suggests that materiality assessment remains a matter of judgment for firms, there is a clear appetite for a more streamlined approach to determining materiality, specifically that this aligns with the materiality definition proposed in SS2/21 pursuant to 5.1A and the FCA's proposed definition under 4.12 to CP24/28.

60. The definition of materiality implies an assessment to determine whether a third-party reaches the definition. With regards to a firm's ability to scale up the third-party service, it would be helpful to understand what regulators expectations are regarding this assessment.

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

61. UK Finance's primary concern centres on the divergence between the PRA's and FCA's approach to the notification requirements. We explicitly advocate for alignment between these regulators and specifically would welcome the PRA aligning with and adopting the FCA's approach to notify *all* material third party arrangements. Whilst we appreciate the PRA's inclusion of an additional threshold for notification of material third party arrangements, and note that this may have the effect of narrowing the scope of notifiable arrangements, it has the practical impact of adding further complexity to reporting practices and additional considerations for firms in determining whether to notify a material arrangement. The desire for regulatory consistency stems from practical considerations about implementation efficiency and the need to minimise administrative burden.

62. UK Finance seeks clarity on the application, particularly regarding Enhanced scope SMCR firms. UK Finance requests that the authorities consider whether the application of these requirements to all Enhanced scope firms may be proportionate. We request that requirements should instead be tied to specific regulated activities rather than firm classification. Some members point out that firms not holding client money or operating in sectors with limited potential for intolerable customer harm might face unnecessary regulatory burden. Members specifically reference section 1.7 of the consultation paper, suggesting the FCA should focus on firm types rather than maintaining a broad Enhanced Firms categorisation.

63. The practical aspects of notification templates require clarification. UK Finance seeks confirmation about whether the same template will serve both Material Third Party Notifications and the Annual Material Third Party Register. Using identical templates for both purposes might present some challenges in that certain information may not be available at the time that firms are required to notify of new material arrangements. CP24/28 states that firms should notify the regulator of new material third party arrangements 'before' making any internal or external commitments. Members seek clarity on what is meant by "internal commitments".

64. Under the amendments to SS2/21 firms are expected to notify regulators upon initiation of or change to a contract with a material third party. It is worth noting that some major suppliers may not (indeed, have not to date) committed to specific timeframes for supporting the notifications required by the regulators. If the PRA requires a notification upon occurrence, then there may need to be some requirements directly on suppliers to enforce this.

65. The volume of notifications under the new framework presents another area of concern. The inclusion of all material non-outsourcing arrangements is expected to

increase reporting volume significantly and UK Finance highlight the industry's desire for streamlined reporting processes.

66. The proposed regime will almost certainly result in better visibility for the authorities for concentrations being formed around certain suppliers. UK Finance would welcome proposals by the authorities to provide this visibility back to the sector so that firms can better understand where those concentrations exist and mitigate the risk that these present.

67. UK Finance suggests that while the industry understands the regulatory objectives behind enhanced notification requirements, the key to successful implementation appears to lie in achieving greater regulatory alignment and establishing efficient reporting mechanisms that minimise duplicative efforts while maintaining effective oversight.

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

68. On the technical implementation side, members highlight some concerns regarding the platform choice for submissions. Some members note that while the material outsourcing register is currently reported through the Bank of England's BEEDs system, the proposed dual-regulator reporting structure may necessitate a different approach. The PRA consultation paper suggests RegData as the reporting platform, which some members view favourably given its existing use for other regulatory returns. However, some members have not had access to the platform so are unable to comment on its practicability.

68.1. To supply an example, for one Member, in 2024 the submission was hundreds of thousands of rows (incl. Internal outsourcing). With the addition of material non-outsourcing, this is estimated to increase by half again. Some members note that they will still be impacted by the multiples challenge as the templates shared do not appear to be the relational database structure expected.

69. UK Finance question the necessity of certain information requests. The new reporting template requires information on firms' due diligence conducted for each arrangement, including details on risk assessments, recent audits, and governance reviews. UK Finance advocates for a proportionate approach to ascertaining this information.

70. Given the overlap with the Supervisory Statement on Critical Third Parties to the UK Financial Sector, where the information submitted will be used for identifying and regulating the CTPs, it would be helpful to understand what efforts are being made to reduce duplicate reporting.

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

71. UK Finance emphasise the importance of having a single, unified template that satisfies both PRA and FCA requirements. Currently, the consultation papers present different templates for third party data reporting, creating potential confusion and inefficiency.

In particular we note the following points of divergence:

- Whilst the overall number of datapoints in the PRA and FCA template align, the templates themselves do not align. In particular, we note that:
 - The PRA template has 6 tabs whilst the FCA's has 7 tabs
 - The data fields in Tab 7 in the FCA template are part of another tab in the PRA template
 - Reference numbers do not align for 25 datapoints
 - Certain datapoints have slightly different names

72. The technical aspects of template implementation raise several practical concerns. UK Finance's primary concern is that the template uses multiplicative data rows, each selection is a new data row, which makes files unwieldy and unusable. Members specifically request that cell locking, and controls be used sparingly to facilitate bulk text input where appropriate. UK Finance also strongly advocate for the inclusion of a compliance tab, noting the utility of such guidance in previous outsourcing register templates. These technical considerations reflect the operational reality of managing large-scale regulatory reporting.

73. The reporting format for impact tolerances in fields 3.18 to 3.22 requires expressing impact tolerances in hours. This approach fails to account for volume, value, or other impact measures, potentially creating misalignment with SS1/21 and disadvantaging firms with more sophisticated operational resilience frameworks.

74. Members have commented that the current format of voluntary reporting is challenging to work with which makes it a resource intensive exercise for smaller firms. This is particularly challenging where duplicate lines are required to capture all combinations of suppliers, subcontractors and alternative providers. UK Finance advocates for the removal of this requirement for duplicate lines in the finalised template.

75. The matter of validation and data quality emerges as another key consideration. UK Finance suggests incorporating built-in validation checks.

Additionally – The following issues are noted with the respective areas:

ID 3.07 – Date of service commencement seems to be a duplication to Date of contract commencement

ID 5.01 - Supply Chain Ranking: The supply chain ranking does not substantively add value to risk management as financial entities identify and manage the risks associated with material subcontractors irrespective of their position in the subcontracting chain. It may also be operationally challenging to execute given that many members do not have this in place at this juncture.

ID 6.06 - Outcome of the most recent audit – Would like to understand if the response of "not done" is expected for on-going audits (at the point of reporting), where outcome is not completed/ not known.

76. The industry assumption had been that firms would submit once to the RegData Platform for both the PRA and FCA. Given the differences in the templates standardisation is required to ensure that firms do not need to populate two templates with the same information to be uploaded twice.

77. Finally, UK Finance would welcome clarity from the regulators regarding the process and timelines that will be followed should there ever be a change to the template. It would be useful to have surety that there will not be a sudden, unexpected change – particularly in a period when registers are being compiled for submission. For firms to fully automate their registers they will need more than the current c.3 months' notice of change so that new/changed fields can be implemented.

PSD2 Commentary

Throughout this response, UK Finance has set forth Member commentary on the interaction between the Payment Services Directive 2 (PSD2) reporting requirements for UK financial institutions and the proposed new incident reporting frameworks. The aim of this section is to bring these points together for clarity.

78. UK Finance members have identified several key concerns regarding the continued existence of PSD2 reporting requirements that warrant serious consideration by regulatory authorities.

79. A fundamental issue is the regulatory duplication created by maintaining PSD2 incident reporting alongside the new proposed operational incident framework. As explicitly noted in the FCA's consultation paper clause 3.53, these new requirements do not replace PSD2 obligations, potentially creating burdensome parallel reporting structures. This duplication places UK financial institutions at a competitive disadvantage compared to their European counterparts, who benefit from the consolidation of reporting requirements under the Digital Operational Resilience Act (DORA). The cost-benefit analysis in the consultation fails to adequately account for this regulatory overlap and the associated compliance burden.

80. The practical implications of this duplication are severe. For example, one member firm reported having to submit fifteen intermediate reports under PSD2 for a single incident. Under the proposed combined regime, this same scenario would require approximately thirty separate reports with competing deadlines across PSD2, the new UK incident reporting framework, and informal updates to supervisors. This level of compliance activity diverts significant resources away from actual incident management and remediation, undermining the primary objective of these frameworks.

81. PSD2 reporting has particularly stringent timeline requirements, with initial reports due within 4 hours of incident detection. When combined with the new proposed requirements, firms face a complex web of reporting obligations with different thresholds, timelines, and data requirements. This complexity is further exacerbated for dual-regulated firms, which must navigate as many as five different reporting regimes across the PRA and FCA, often with competing criteria and internal governance structures.

82. UK Finance and its members strongly advocate for the repeal of PSD2 incident reporting requirements in conjunction with the implementation of the new framework. This could be achieved through a statutory instrument repealing "The Payment Services Regulations 2017, SI 2017/752, Part 7, Regulation 99" or through the FCA providing waivers or modifications allowing non-compliance with these specific rules. A streamlined approach would not only reduce the administrative burden on firms but would also allow for more focused and effective incident management.

83. The timeline considerations between the two regimes create additional challenges. While PSD2 has the 4-hour initial reporting deadline, the new framework proposes a 30-

working-day deadline for final incident reports—a timeframe that many members consider insufficient, particularly for incidents involving third parties where root cause analyses depend on external providers. This creates a situation where firms must juggle short-term PSD2 requirements alongside potentially conflicting timelines in the new framework.

84. The current PSD2 reporting structure also contains elements that are being reconsidered in other regulatory contexts. For instance, European lawmakers removed certain data fields from the Regulatory Technical Standards for major incident reporting under DORA, recognising their impracticality. The Financial Stability Board is similarly reevaluating some of these requirements, indicating that the PSD2 framework may contain outdated or impractical elements that should not be perpetuated.

85. UK Finance recognises that the regulators have considered reducing the regulatory burden by not enforcing intermediate reports in the new framework. However, this benefit is largely negated by the continued existence of PSD2 reporting requirements. A more effective approach would be to establish a single, unified reporting regime that incorporates the best elements of both frameworks while eliminating duplication.

86. To achieve a truly effective incident reporting structure, UK Finance recommends that the PRA and FCA:

- Support the implementation of a statutory instrument to repeal PSD2 reporting requirements before the implementation deadline of the new framework, or provide a waiver to PSD2 reporting for all payment service providers operating in the UK.
- Create a single reporting approach that aligns with international best practices and the operational resilience framework already in place for many financial institutions.
- Ensure that supervisory teams are instructed to reevaluate and cancel any informal reporting agreements with firms, except where a clear justification exists, to prevent further reporting duplication.
- Consider the international competitive implications of the UK's reporting framework, particularly compared to jurisdictions that have streamlined their requirements.

87. By addressing these PSD2-related concerns and implementing a more streamlined approach to incident reporting, regulatory authorities can significantly reduce the administrative burden on UK financial institutions while maintaining effective oversight. This would align with the government's stated objective to "make regulation work much better for our economy" and support the recalibration of financial regulation to balance risk management with growth considerations.

Summary

In summary, whilst UK Finance appreciates the PRA's and FCA's efforts to enhance operational incident reporting and third-party risk management, we highlight several areas requiring significant refinement.

- **Cost and Burden Concerns:** The proposed regime underestimates financial and resource burdens, with firms likely facing substantially higher DORA costs than the consultation suggests. Parallel reporting obligations, particularly PSD2 incident reporting, create unnecessary duplication, which must be addressed.
- **Operational Incident Definitions and Thresholds:** The overly broad definitions create serious risk of excessive and unnecessary reporting burdens. Terms such as 'potential impacts,' 'operational contagion,' and 'indirect impacts' introduce unacceptable levels of subjectivity and complexity that directly compete with existing incident management priorities. The inclusion of criteria like 'could cause harm' sets an extremely low threshold that will inevitably lead to over-reporting and divert resources away from actual incident remediation. The proposed definitions fail to acknowledge the practical realities of incident management, where information scarcity in early stages makes speculative assessment of potential impacts particularly problematic. Equally concerning are requirements to report on legal/regulatory non-compliance and reputational impact, which force firms to engage in counterproductive speculation during critical incident response periods. UK Finance urges immediate realignment with existing operational resilience regimes and recognition of firms' internal classification systems as the foundation for a more proportionate, outcomes-focused approach.
- **Standardisation and Reporting Proportionality:** The lack of regulatory alignment between the PRA and FCA increases reporting burdens. UK Finance strongly supports the repeal of PSD2 reporting and calls for a single, unified reporting approach.
- **Third-Party Risk Management:** While the focus on material third-party arrangements is welcomed, the inclusion of non-outsourcing relationships expands reporting obligations excessively. The regulators must provide further clarity on the proportional application of these requirements.
- **Implementation and Templates:** The misalignment of reporting templates, the lack of a unified submission structure, and the excessive data collection expectations create operational inefficiencies. UK Finance calls for a streamlined, proportionate approach.

We strongly encourage regulators to engage further with industry stakeholders to ensure that these proposals enhance resilience without imposing unnecessary regulatory burdens. UK Finance remains committed to working collaboratively with the PRA and FCA to refine the final framework in a way that achieves practicality, proportionality, and regulatory effectiveness.