FIA.org

FIA Response to consultation on operational incident, outsourcing and third-party reporting

FIA appreciates the opportunity to provide feedback on this Consultation Paper (CP). FIA notes that there are a few high-level comments and observations that apply to many of the sections covered by the FCA, PRA and BoE in their respective CPs, and we detail at the outset of our reply. We also cover these topics within the answers to each specific section where they apply.

1. Overarching comments

Alignment between BoE/PRA CP 17/24 and FCA CP24/28

FIA understands from the CPs that the PRA, FCA and BoE have closely collaborated on the rules laid out. However, on closer reading there appears to be some differences for which FIA recommends, throughout its response, for additional evaluation and adjustments. Acknowledging that some divergence may be necessary consistent with the regulators' respective mandates and objectives, FIA advocates for increased convergence of the rulebook, handbook and Supervisory Statements (SS). The operational burden felt by firms will be during the triage phase to determine whether an incident meets the initial threshold and assessment criteria. Maintaining two, distinct regimes between the FCA and PRA therefore increases the complexity at this early stage. One member, for instance, triages nearly fifty incidents per one reported incident.

Proportionality

FIA welcomes the regulators' focus on creating a risk-based and proportionate framework, particularly the decision to limit the register and notification requirements to material third parties. This approach helps maintain an effective balance between oversight and operational efficiency, reinforcing risk-based risk management practices. Our feedback aims to highlight areas where the requirements could be further refined to better align with a genuinely risk-based model. Strengthening this alignment would ensure regulatory efforts remain targeted at managing key risks while avoiding unnecessary administrative complexities.

PSD2 and PRA/FCA Reporting

The FCA notes in Section 3.53 that PSD2 will remain in effect within UK legislation and the FCA handbook. As per the removal of PSD2 reporting under DORA, the FIA's position is that multiple and duplicative incident reporting regimes should not be maintained within individual jurisdictions. The UK is able to remove the relevant Article within legislation via a statutory instrument. The FCA, in addition, could propose a waiver for the sector which would allow all firms to report via the new proposed regime. This ensure that the UK remains competitive via-a-vis other jurisdictions and that the cost to do business remains low. There is a risk that the intermediate reporting phases would become overly burdensome due to the indiscriminate nature of intermediate reporting phases in PSD2 and the UK proposal. One member has experienced fifteen intermediate reports, which would result in thirty reports once the new UK proposals come into effect.

The existence of separate reporting requirements for PRA and FCA-regulated firms risks adding further complexity and redundancy. FIA welcomes additional clarity on how firms should determine their reporting obligations when an incident meets both PRA and FCA criteria. Since all incident reports will be submitted through the same FCA portal, dual-regulated financial institutions would appreciate further guidance into how incident reports should be coordinated. This is notable in relation to the reporting trigger field included in the

formatting, as each report would relate to the initial trigger (which informs the regulators whether the report is FCA or PRA). This would be especially helpful for incidents that could trigger reporting for all of the following rules: 1) the proposed PRA regime, 2) the proposed FCA regime, 3) FCA Fundamental Rule 7, 4) PRA Principle 11, and 5) the FCA's PDS2.

Operational Contagion

The PRA has expanded the concept of operational contagion within its incident reporting rules, following its introduction by the Financial Policy Committee (FPC). This concept, along with financial contagion, has now been incorporated into the FMI Fundamental Rules and the final rules for Critical Third Parties. However, the term and the broader expectations around operational resilience in the UK have not been subject to industry consultation, making their implementation unclear and potentially complex. The sector strongly supports a formal consultation process and industry engagement before this concept is embedded into regulatory frameworks.

Furthermore, there is a lack of clarity on how firms are expected to incorporate financial and operational contagion into their incident management processes. The FPC's requirements suggest firms must assess how an incident could affect the real economy, the financial sector, households, and businesses. This includes determining whether third parties—such as households—could face liquidity shortages, lack alternative capabilities, struggle to access funding, or experience difficulties with price discovery and margin payments. However, financial institutions have limited ability to assess third-party financial health, particularly in relation to the short-term impact of an operational incident. While the sector recognises the role sectoral and wider economy impact, this should not be determined within the short timeframe available between incident origination, remediation and initial reporting.

The above considerations are equally applicable to the FCA's use of 'indirect impact' and 'potential' incidents. The financial sector recognises that incident reporting serves a function for regulators to be able to understand whether they need to intervene. Reporting, therefore, should be based on realised incidents and on tangible information that relates to the specific incident. Subjective analysis, regarding wider sector impact or an unrealised incident impact, neither serves the objective of informing the regulator whether intervention is required nor improves a firm's remediation of the incident. FIA notes that a large proportion of FCA regulated firms are not subject to the operational resilience regime. It is unclear if these firms have the sophistication or mature enough incident management operations to appropriately consider indirect impact. FIA supports are more simplified regime across the PRA and FCA.

Reputational Impact

While firms acknowledge that reputational concerns are important to regulators and, in some cases, require transparency, there is a growing risk of threat actors exploiting these requirements. Attackers have increasingly used fabricated incidents and media outreach to manipulate market reactions.

The current reputational impact criteria cover a broad range of incidents with varying degrees of severity. Firms recommend reassessing these criteria to ensure that incidents are only reportable based on reputational damage when they result in an inability to provide adequate services. For instance, an incident that leads to social media speculation or local news coverage may have a minor impact, whereas losing clients or

counterparties with a "material impact on business" is significantly more consequential. The reporting framework should better distinguish between these scenarios.

FCA Case Study-Based Criteria

While the FCA's use of case studies provides insight into its expectations for operational incident reporting, it also introduces inconsistencies in how incidents are classified compared to the PRA. For example, one case study suggests that an incident affecting “some” clients and disrupting any aspect of “day-to-day management” would be reportable, as would an incident where a website is taken offline without considering the availability of alternative banking services via an app, Post Office, or phone.

Additionally, there is a stark difference in the severity of incidents covered by the case studies. For example, case study 8 describes a complete IT infrastructure outage for a digital bank, whereas case study 5 references a website being offline. FIA recommends greater consistency in how incident criticality is assessed across the FCA and PRA frameworks. Small incidents, or those with high levels of media focus, will likely be reported to supervisors under FR7 and FIA supports realised incidents being supported under the incident reporting regime only. Greater delineation and clarity should be provided regarding the difference between supervisory expectations and incident reporting.

Legal and Regulatory Non-Compliance

Firms are concerned that including legal and regulatory non-compliance as an incident threshold could lead to speculative reporting. This may require firms to assess potential breaches of contracts or regulatory requirements, which they may not be comfortable hypothesizing within a regulatory report. Notably, similar reporting fields were removed by European lawmakers from the Regulatory Technical Standards for major incident reporting under DORA (the “Incident Reporting RTS”). The consultation paper for the Incident Reporting RTS initially included fields such as “inability to comply with legal requirements” (4.4), “breach of contractual arrangement” (4.5), and “amount of fees due to non-compliance with contractual obligations” (4.18), but these were ultimately excluded. Firms therefore recommend removing this criterion from incident reporting requirements.

Internal Classification

The sector welcomes the PRA’s recognition of internal classifications when determining if an incident is reportable. A number of financial institutions have agreements with regulators to share incidents above a certain internal classification threshold, to which no complaints have been received. The sector believes this model could be effective and, alongside guidance regarding what factors could be considered and the mandates of the respective regulators, could offer a practical and simple regime for firms to follow. The PRA and FCA should both place internal classifications at the same level as their regulatory thresholds to allow for an outcomes-focused regime where firms can match their internal levels to the regulator’s mandates. Maintaining consistent and global classification levels is good cybersecurity practice as it allows for effective escalation and crisis management. If the regulators or supervisors remain concerned with a lack of reporting or missed notifications after one or two years of compliance, the regulators can follow-up with a further Consultation Paper or guidance regarding threshold levels. Regulators, in addition, have demonstrable powers to intervene on a firm-by-firm basis should underreporting continue.

A concern though remains regarding the need to apply a consistent judgment on incident notifications. The focus on incidents that "could" cause harm is overly broad, and likely to lead to significant overreporting. Given the regulators' desire to align with international standards where possible, it should be noted that under DORA firms apply the notion that they notify the regulator in line with the normal workflow once an incident is recognised as major – rather than applying a judgment call throughout the incident lifetime.

2. Operational Incidents

Paragraph (P) 2.4 current text: *The operational incident reporting proposals would apply to the reporting of an 'operational incident', which is defined as either a single event or a series of linked events which disrupts the firm's operations such that it:*

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

FIA Comments:

The current definition is too broad and does not adequately address the various levels of disruption that can occur. This could potentially lead to an over-reporting of minor incidents, which might not be necessary for the stated-aims of the reporting rules.

FIA recommends greater consideration is given to the thresholds for reporting and a refining of the operational incident definition itself, which should instead be limited to important business services to avoid creating a complex regime that does not focus on the most important risks. This would also be in line with existing UK operational resilience regime and DORA, where Critical Important Functions (CIFs) are the relevant service level. FIA recognises the FCA's statements regarding firms that are not subject to the operational resilience regime and would support recognition of important business services alongside a proportionality statement for firms who will not have mapped their services.

FIA seeks clarification and recommends the "**or**" between the clauses in P2.4 (bolded above for emphasis) should be an "**and**". Alternatively, FIA would recommend the second clause in P2.4 to be removed from the drafting. The PRA risks becoming the ICO for non-personal data as this is too broad. The focus on confidentiality, integrity, availability (CIA) would lead to overreporting and may obscure reference to operational impacts.

3. Important Business Services

P2.12 current text: *The PRA would expect firms to report incidents meeting the thresholds set out in the PRA rules, even if these have not yet breached the impact tolerances of any affected important business services. As set out in paragraph 2.9, firms would need to assess whether operational incidents, which do not initially impact important business services or breach impact tolerances, could pose a risk on the PRA's statutory objectives and, in the case of O-SIIs or relevant Solvency II firms, financial stability.*

FIA Comments: FIA welcomes further clarification as we understand that firms would only report Important Business Service related incidents as only they are likely to pose a risk to the PRA's statutory objectives. The above statement risks detaching the incident reporting regime from the resilience regime that the UK has implemented. FIA recognises statements from the PRA regarding an incident that could affect 'multiple services at the same time that are not important business services', however, note that this example is highly unlikely to impossible to occur. The statement in P2.12 to remove the regime from existing rules should not be predicated on an edge case which is highly unlikely. PRIN 11 reporting is expected to remain and should therefore encapsulate incidents that are edge cases and impact the PRA's mandates (which is a high bar for incident impact).

4. Third Parties

P3.7 current text: The PRA proposes to define a 'third-party arrangement' as any arrangement whereby a person provides a product or service to a firm whether or not this would otherwise be undertaken by the firm itself, provided directly or by a sub-contractor, or provided by a person within the same group as the firm.

FIA comments: Regarding the inclusion in the definition of "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.

5. Material Third Parties

P3.7 current text: *The PRA proposes to define a 'third-party arrangement' as any arrangement whereby a person provides a product or service to a firm whether or not this would otherwise be undertaken by the firm itself, provided directly or by a sub-contractor, or provided by a person within the same group as the firm.*

FIA Comments:

FIA recognizes the reasoning behind broadening the scope to include both outsourcing and non-outsourcing arrangements to address the broader network of third-party dependencies. However, the definition of 'third-party arrangements' now covers a significantly wider range of third-parties compared to existing requirements in other jurisdictions, such as those focus specifically on ICT-related risks. This has raised concerns among firms about potentially to capturing an overly broad set of relationships, which may shift focus away from critical risks and lead to excessive reporting.

To enhance the effectiveness of the chosen scope, we suggest refining the scope to cover only products and services delivered "*on a recurrent or ongoing basis*" in line with the FSB Toolkit and DORA.

Additionally , to ensure that a materiality threshold is appropriately applied to the definition of "material third-party arrangements", we suggest that the regulators replace "pose a risk to" with "materially impair". The proposed use of "pose a risk to" lacks a materiality threshold which carries certain implications for firms risk assessments and risks capturing an overly broad population of material arrangements. By contrast, the term "materially impair" captures those arrangements that could have a tangible, rather than merely a theoretical, potential for harm. This approach would seem to align with the regulators' intended objectives to capture those arrangements that truly warrant their attention.

FIA seeks additionally clarity on the treatment of intragroup arrangements. Due to the different language used by the PRA (SS2/21) and by the FCA on what they expect to be considered material third party arrangements, there is a risk of having a dual reporting regime where the PRA and FCA differ on the materiality of the same third party arrangement (e.g., intragroup arrangements). FIA would encourage the PRA and FCA to align on what third party arrangements should, and should not, be considered material.

FIA notes that possible confusion may arise from the inclusion of 'person' to be used to describe a third party arrangement, rather than 'external entity' or something similar. This is likely to lead to differing interpretations of what constitutes a third party arrangement.

Suggestion: *'third-party arrangement' as any arrangement whereby a person provides a product or service to a firm ~~whether or not this would otherwise be undertaken by the firm itself~~, provided directly or by a sub-contractor, or provided by a person within the same group as the firm.*

6. Summary of Costs and Benefits

P1.24 current text: *In summary, the PRA estimates an upper bound of one-off and ongoing (annual) compliance costs of £11,382,000 and £858,000 respectively aggregated across all firms in scope of the proposals.*

FIA Comments: The PRA's implementation cost estimate might be too conservative. Incident reporting to a standard rather than ad hoc is a positive development but will mean uplifts that need delivery and governance (and the risk associated with failing to meet detailed expectations). The act of reporting constitutes a high level of governance and often requires approval of each report by SMF24-level executives. A minimal estimation of the time required for approvals due to a high-level of executive time would likely result in higher costs. The operation burden at a working level if found at the beginning of the triage process where incidents are evaluated according to the regulator's thresholds and assessment criteria. This often requires multiple teams alongside incident management. The PRA's analysis should add this expectation with calculations reflecting the member input that each reportable incident has approximately fifty triaged incidents that were not deemed reportable. The lack of inclusion of the FCA reflecting another regime or PSD2 is a gap in the cost benefit analysis. We also note the PRA register template will require an uplift compared to the existing template.

7. Notifications

P3.2 current text: *The PRA has considered how to standardise the way firms submit material third-party notifications and proposes to require firms to submit this information in a template, supported by additional documentation where necessary. The introduction of a standardised template aims to provide clear expectations on the minimum information expected in material third-party notifications and reduces firms' reporting burden.*

FIA comments:

Scope

We recognize that the FCA and PRA have taken broadly aligned approaches, with some necessary differences to meet their respective oversight objectives. However, we are concerned about certain inconsistencies that may introduce unnecessary complexity for firms. A key issue is the variation in how third-party arrangements are defined: the PRA requires notification of *"material third-party arrangements which, due to associated risks, necessitate a high degree of due diligence, risk management, or governance by the firm."* Meanwhile, the FCA mandates notification of *"all material third-party arrangements"* without further clarification.

This discrepancy creates challenges in implementation and reporting. While we appreciate the PRA's intent to provide clearer guidance and a more focused scope, the approach ultimately increases complexity without significant benefits to risk management or a risk-based framework. In this regard, firms would prefer the PRA to align with the FCA's simpler framework, which would also be more consistent with the PRA's complementary policies.

Under the amendments to SS2/21 firms are expected to notify regulators upon occurrence of a change or initiate 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.

Template

There is uncertainty among firms regarding the intended use of the notification template. The PRA has stated that the proposed templates for notifications and registers are designed to be aligned. However, this has been interpreted as requiring the register template to be used for notifications, which would be impractical. It would appear that Appendix 6 (template) is intended for usage for both Registers and Notifications. A separate template for this might be easier.

At the time of notification, certain data fields—such as the contract execution date—may not yet be available, making the process unfeasible. To ensure clarity and ease of implementation, we request further guidance from both the PRA and FCA on how firms should use the proposed templates for notifying arrangements. In particular, firms would like explicit confirmation that they will not need to resubmit the entire register every time a notification is required as this would cause significant operational burden with no added benefit to regulators.

Subcontractors scope

We appreciate the regulators' decision to limit reporting requirements to subcontractors *"whose disruption will impair the continuity of the firm's service."* To ensure a truly risk-based approach, we recommend refining this definition to focus on subcontractors ***"whose disruption would materially impair the continuity of the firm's material third-party service."*** This revision recognizes that not all subcontractors linked to a material third-party service have the same level of significance or potential impact on service provision.

Subcontractors ranking:
The requirement to "rank" the subcontracting chain does not provide meaningful value for risk management or supervision. It does not align with how firms typically manage supply chain risks, which involves identifying and mitigating risks associated with “material” subcontractors regardless of their position within the chain. Additionally, ranking all subcontractors presents operational challenges for firms.

These concerns were previously raised in advocacy discussions related to DORA, and we strongly encourage regulators to depart from the DORA approach in this regard. However, if UK regulators decide to retain this requirement, we urge full alignment with DORA’s methodology for intragroup providers. Assigning a rank of 0 to intragroup providers overlooks the reality of complex subcontracting structures. In such cases, it remains unclear how firms should rank intragroup subcontractors—under the current approach, all intragroup subcontractors would default to 0 until the first external provider is identified, which may be located much further down the chain.

8. Register

P3.28 current text: *To minimise firms’ reporting burden, the PRA has developed the proposed templates for the Notifications and Register to be aligned with one another. The PRA has developed the templates predominantly using the existing Register templates that have been used for previous PRA Outsourcing Register data collections as a basis. To provide consistency and reduce reporting burden on firms, the PRA has developed its proposed templates to be interoperable where possible with similar existing and future regimes, such as the EBA Outsourcing Guidelines and Article 28 of the EU’s DORA.*

FIA Comments: We welcome the use of a standardised template, but would ask that the PRA and FCA align templates perfectly as the differences are minimal but will create additional operational burden for firms. We would also ask that the PRA and FCA outline the process and timelines they will use if there were ever to be a change to the template. It would be useful to have the certainty that there will not be sudden, unexpected changes particularly in the period when registers are being compiled for submission. For firms to fully automate their registers they will need more than the current 3 months’ notice of change so that new/changed fields can be implemented.

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 (noted below), standardisation is required to ensure that firms do not need to populate two templates with the same information to be uploaded twice. This includes minor (one word) differences in definitions which though small add uncertainty without delivering any tangible benefit. Equally the numbering of fields differs across the registers where again, a one-for-one template would facilitate more efficient reporting.

The register template carries forward the current row-per-dropdown approach which is onerous, leading to >200k data rows per submission. Every additional multi-select data field adds to this. Consequently, files become so large the must be split in order to allow compilation and editing. This is in contrast with the ECB/DORA register. We would urge for a simpler data structure, where possible.

As proposed in section 5 (Material Third Parties), we note that in the FCA CP , the second limb of the definition of Material Third Party Arrangements is similar to, but different from, the definition the FCA uses in SYSC 15A. We recommend to ensure the second limb of the definition of Material Third Party arrangements is the same as the second limb of the SYSC 15A definition of Important Business Services.

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.

Simplification recommendations on the Register template

FIA notes that the total number of datapoints in the PRA and FCA template align. However, the templates themselves do not align and we note for the attention of the regulators that:

- The PRA template has 6 tabs while 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 differ slightly in their names

- **ID 3.11** – description of changes made to the contract is unnecessary; these will be reflected in the template as the details of the engagement are updated.
- **ID 3.06-3.06 –** requires date of contract commencement and service commencement; burdensome and unnecessary, the service commencement date is not always known at the time of contract commencement date and may vary depending on location etc.
- **ID 3.20-3.24 –** data fields requiring information on impact tolerance are broken out (diverges from DORA approach; TBC whether feasible to provide this information.
- **ID 4.03 –** LEI is required for TP but guidance to enter N/A if you cannot find TP in the look up tab is unclear; further clarity may be required here
- **LEI:** We do not consider the requirement to provide an LEI when identifying an alternative supplier is necessary or proportionate. For instance, whilst we may know the supplier we may not know the particular entity at this stage.
- **Type of Service / Service Category:** The terminology used here (i.e. use of "service" for both taxonomies) creates some confusion. FIA understands 'Service Category' to be a legacy taxonomy from the previous template, however it may be helpful to revise this to "Function Category" to distinguish it from the "Type of Service" taxonomy and reflect its relation to the business or corporate function (i.e. the IBS category).
- **Contract / Arrangement Ref Number:** The 'contract reference number' (a key relational field) is required in the second template (**ID 3.01**) but it appears there is no unique identifier that connects the various tabs of the templates. This might be addressed in the final templates, however necessary to flag that the contractual reference number should be added to every tab (except for the first two tabs). Related to this, the template also calls for an 'arrangement reference number' (**ID 3.02**). This should not be necessary given that entities will now be providing a contract reference number (which is aligned with DORA register) and should be deleted.

- **Subcontractors:** Whilst it is not explicitly mentioned, we assume that only Tabs 4 and 5 are required to report subcontractor details (this should be clarified if not the case).

Recommendation for optional fields at the notification stage

- **Contract start/ service start date** (ID 3.06 and 3.07): As notification occurs before service commencement, these dates will not be finalised at the point of notification and requiring them could result in firms providing indicative rather than confirmed timelines. The service start date is likely to prove particularly challenging given that the service start date will depend on the notification period having concluded. It is much more likely that the contract execution date will be known, however this is not certain especially when contracting out of the UK.
- **Date and outcome of audit** (ID 6.05 and 6.06): We note that the PRA has asked for both (i) date and outcome of most recent risk assessment, as well as (ii) most recent audit, i.e. distinguishing between both as separate activities. Whilst it would be typical for entities to undertake a risk assessment at onboarding, it would be less likely that entities would be undertaking an audit (despite being contractually entitled to).
- **Function Information** (ID 3.15, 3.16 and 3.17): The assessment of whether the arrangement supports an IBS is typically something which is undertaken on a look-back basis, often long after contract execution.

9. Phased approach to reporting operational incidents

P2.16 current text: *As illustrated in Figure 1, when an operational incident occurs, firms would be required to assess whether it has met a threshold set by the PRA. If a threshold has been met, firms would be required to submit an initial report as soon as practicable. The PRA would expect that firms submit the report within 24 hours.*

FIA Comments:
FIA welcomes tying reports to classification thresholds but we would appreciate further clarification on the preferred approach vis a vis incidents which haven't initially met the threshold. FIA welcomes clarification on whether the Bank of England still expects earlier (heads up) communications. FIA Members currently receive requests for early heads up information prior to breaching any threshold.

Timeline for final report:
FIA welcomes a 60 days extension for the final report to align with firm's internal root cause analyses and reviews.