# CP24/28: Operational Incident and Third Party reporting

## Response to consultation

**About the Investment Association**

The Investment Association (IA) champions UK investment management, a world-leading industry which helps millions of households save for the future while supporting businesses and economic growth in the UK and abroad. Our 250 members range from smaller, specialist UK firms to European and global investment managers with a UK base. Collectively, they manage £9.1 trillion for savers and institutions, such as pension schemes and insurance companies, in the UK and beyond. 49% of this is for overseas clients. The UK asset management industry is the largest in Europe and the second largest globally.

We consent to the publication of the Investment Association’s name on the list of respondents.

**Overall comments**

The Investment Association welcomes the opportunity to comment on CP24/28: Operational Incident and Third Party reporting. We support the intent and spirit of the proposals but are concerned that, as drafted, aspects of the proposals are not the best way to achieve the FCA’s aims. In particular, the proposed reporting threshold for operational incidents has become too complex owing to the lack of alignment with the existing UK operational resilience regime. As drafted, the proposed regime would in practice result in overreporting of low level incidents and ultimately place a disproportionate burden on firms. In our responses we provide feedback and suggestions on how to refine the proposals to make them more practical, proportionate and clearer to interpret. We especially emphasise the need to remove overly subjective criteria from the incident reporting thresholds. Even at this stage, there is considerable confusion within the industry on how to interpret the draft wording of the thresholds. Simplification is essential.

Many of our issues with the incident reporting proposals stem from the deliberate choice to not align with the existing operational resilience policy and the concept of Important Business Services (IBS). We understand that only roughly 5% of FCA regulated firms are in scope of the operational resilience policy and will have performed the exercise of identifying their important business services and setting impact tolerances, and therefore it may not be appropriate for all firms to align to IBSs. Notwithstanding, for those firms who are in scope of the operational resilience policy, and who constitute the greatest risk of any market integrity impact, continuing to align to IBSs is highly desirable.

The CP suggests that the FCA would like to gain insight into incidents not related to Important Business Services. We are not convinced of the need for this. The concept of Important Business Services was designed to focus attention on the services that pose a risk to the regulator’s statutory objectives. If an incident is unrelated to an IBS, then it is unlikely to have the potential to affect the FCA’s objectives. Further, at this stage, firms in scope of the operational resilience policy have designed their resilience programmes around the concepts of IBSs and intolerable harm. It is unhelpful to these firms to be forced into recalibrating those programmes, developed over several years, to accommodate a significantly expanded focus necessitated by these proposals. Insights into non-IBS related incidents could nonetheless be gathered via other methods, such as the continued role of Fundamental Rule 7 (to which the FCA can enforce).

Regarding those firms not in scope of the operational resilience policy, we question whether it is proportionate to include them within scope of the proposed incident reporting requirements. Such firms have fewer resources or sophistication to divert to regulatory reporting during operational incidents and the proposals may impede their ability to remediate issues. Smaller firms will likely have incident management teams ranging from 1-4 employees, who will also likely have other professional responsibilities alongside remediation. Such firms will be less well equipped to perform the analysis necessary to theorise on the potential for an incident to impact the FCA’s objectives. Should the FCA continue with a blanket application of the incident reporting regime, the IA would suggest that the assessment criteria is significantly simplified and places far more emphasis on recognition of internal firm classification.

Considering that all firms are already required to notify the FCA of issues under Principle 11 / SUP 15.3 General notification requirements, we suggest the FCA seeks to address underreporting by firms not in scope of the operational resilience policy by improving compliance with its existing rules, rather than resort, at this stage, to layering on additional rules. This would not prevent the FCA from introducing an incident reporting template to improve data standardisation and issuing guidance on the timeliness of reports. This approach would also clear the way to allow firms in scope of the operational resilience policy to continue aligning to the Important Business Services which their operational resilience programmes are designed around.

To summarise, our top three messages are:

1. New incident reporting requirements should only apply to firms in scope of the operational resilience policy, allowing those firms to continue aligning to Important Business Services. Insights into non-IBS related incidents can still be gathered via other less onerous methods.
2. Simplify the incident reporting thresholds by removing overly subjective criteria. Allow firms to exercise their judgement in relation to the severity of incidents they determine are reportable, to avoid unnecessary overreporting of low-level incidents.
3. Address underreporting among firms not in scope of the operational resilience policy by reaffirming existing expectations and requirements under Principle 11 / SUP 15.3 General notification requirements. These firms can still use the new reporting template to improve data standardisation and can be issued guidance on the timeliness of reports.

**Responses to specific questions**

**Q1: 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?**

The stated benefits to firms expressed within the Cost Benefit Analysis (CBA) are over-estimated, in our view. The FCA and PRA have provided two separate criteria where there is inconsistency between the financial stability threshold of the PRA and the consumer harm threshold of the FCA. This conflation alongside the addition of subjective analysis included in the assessment criteria (operational contagion, indirect impact, potential incidents, sector/client/consumer impact) will result in a material ongoing cost due to the increased disconnection between regulatory reporting and incident management.

We are concerned by the continued reference to ‘monitoring market-wide risks’ and using the incident data to enable future work. Incident reporting should be based on informing regulators and supervisors regarding actionable information that is relevant to the individual incident. Incident reporting for the purposes of data collection, market analysis and trends is of minimal benefit to the sector and there are other forums where the regulators can request this information. Intervening in incident management for data collection misallocates resource away from remediation and management. IA member firms often face multiple Requests for Information (RFIs) for incidents that cause no customer impact and the reporting regime should encourage better supervisory practices.

**Q2: Do you agree with the proposed definition of an operational incident?**

We recommend removing the ‘user external to the firm’ wording from the definition. It is unclear to us what the scope of ‘users external to the firm’ is. Potentially, it could be interpreted as applying very broadly.

If this element of the definition is to be retained, then it should more precisely refer to those external users of the firm’s services under a contract with the firm who are directly impacted by the operational incident. Smaller firms would be unable to undertake analysis that accurately evaluates the impact of the incident outside of their firm.

A simple regime that is more connected to a firm’s internal incident management could further state that an operational incident is one that requires remediation within a firm’s incident management processes.

In line with our feedback in our ‘opening comments’, we recommend the definition is aligned to Important Business Services.

**Q3: 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?**

The proposals, as drafted, introduce too many subjective thresholds for firms to consider before reporting an operational incident. Incident reporting teams sit alongside incident management teams or are one-in-the-same. Remediation of any incident involves data collection, however, for firms this data will always be directly related to the individual, crystallised operational incident. The addition of terms and criteria such as what ‘could’ occur, contagion, indirect impact and, in extreme, when in relation to an incident that has yet to occur, results in the FCA’s (and PRA’s) proposals being disconnected from the incident management of regulated firms. We recommend further simplification of the thresholds and a removal of all the subjective criteria stated previously. Further, to ensure that the new requirement is applied proportionately in practice, the final policy should explicitly allow for firms to exercise their judgement in relation to the severity of incidents they determine are reportable. This will help to achieve the FCA’s stated aim of targeting only those incidents with a significant impact on the FCA’s statutory objectives.

The current phrasing of 15.18.4(1) does not provide sufficient clarity as to whether an incident should be reported and provides a very open-ended scope. We take particular issue with the ‘could’ in ‘could cause or has caused intolerable levels of harm to consumers’. Given that the degree of harm caused is often strongly linked to the incident duration and this is unknown at the time of occurrence, any operational incident could in theory result in intolerable harm, and thus lead to reporting on every incident.

To take an example, certain operational incidents may result in a firm not being able to use a particular trading system for a short period (sub-30 mins and there may be interim or manual workarounds that do not materially impact customers). The firm would not deem this to be intolerable harm but, were it to persist for a much longer period, this could be interpreted as such. However, at the time of occurrence, it can be hard to predict how long resolution will take, so it is very difficult for firms to ascertain what to report or not.

To give another example, there was an outage with a data provider that a firm’s investment teams rely on and which is updated monthly. The incident occurred and was fully resolved between these data updates, so there was no impact. However, if the firm is to apply the ‘could’ lens, and consider if this might have occurred when a data update was needed and persisted for some time, it becomes an incident that may be reportable. This, however, we would consider to be excessive reporting, be unlikely to provide the regulator with valuable insights and would have not required supervisory intervention to aid the incident. Firms would also still be obligated to provide a general notification under Principle 11.

Both examples would become materially more complex once a firm is expected to consider indirect impact or operational and financial contagion. The firm would then be required to triage both incidents according to an unknown impact to the wider client base or sector. Both subjective analyses would not be related to incident remediation and would be based on information that will be estimates-only. It is unclear why this is required and what further information would be relevant to the regulator. Equally, unrealised impact information appears outside of the scope of supervisory intervention, and it is unclear how the information is going to be used.

We object to undertaking the following triage activity for a ‘potential’ incident or an incident that has yet to crystallise. This triage would be entirely estimates and completely separate from any incident management process. It is unclear how firms would be able to comply effectively nor how any of the information used could be useful for the regulatory authorities. The people who would need to be involved are also the same people who will be tasked with handling the incident itself (developers, product owners, incident response team), detracting from their ability to resolve the incident as soon as possible. The FCA appears to be trying to embed supervisory notification-based concepts (such as informing supervisors of something they should be aware of) into the assessment criteria despite supervisory notifications not being removed when the incident reporting requirements come into effect. These should be separated, with indirect, potential, or press being expected in supervisory notifications and not incident reporting due to the lack of crystalised customer impact.

To avoid unnecessary overreporting and ensure the requirements are proportionate, a certain level of disruption should be deemed acceptable, especially given the FCA’s own definition of operational resilience assumes that disruption is inevitable. Otherwise, this will place a significant reporting burden on firms (particularly given their length; see question 4) if every minor incident is deemed reportable.

The inclusion of incidents the severity of which is ‘low’ in the Initial Report template suggests that a very low bar for these incidents is being set. We would thus advocate for it to be made much clearer that firms can exercise their judgement in relation to the *severity* of incidents that are to be reportable (in addition to our recommendation that the subjective criteria in the reporting threshold are replaced with less open-ended wording).

The CP, at 3.13, acknowledges the link with the existing operational resilience policy and equates the thresholds with ‘impact tolerance’. This is expanded upon in 3.14 to highlight the difference in this CP to the operational resilience policy is the need to notify of potential for breaches rather than actual realised breached impact tolerances. In the definition it would be preferable to use impact tolerance in a defined way as it is in the operational resilience policy.

Moreover, in line with our feedback in our opening comments, we recommend that the new incident reporting requirements are aligned to Important Business Services and apply only to firms in scope of the operational resilience policy.

We also note that the proposed rules overlap with existing reporting obligations, which we see as more pragmatic:

* Breaching Impact Tolerances: as noted in the CP, SYSC 15A.2.11 requires firms to notify the regulator if breaching an impact tolerance. The ‘could’ language supplants this and effectively creates an additional ‘pre-impact tolerance breach’ threshold, which seems unnecessary and contrary to the original operational resilience framework. We are confused that the CP provides thresholds that are directly aligned to operational resilience thresholds for Important Business Services and then refutes this later as applying more widely.
* SUP 15 rules: firms already have a broader obligation to notify the regulator for any material events or rule breaches, so these new proposals would likely mean the additional reporting of only minor, non-material incidents.

Additionally, we have identified further issues with the current reporting threshold proposal:

* The criteria for reputational impact includes a wide range of criteria that would constitute a wide divergence in incident impact. Further, predicting whether an incident will result in reputational impact is not practicable, nor a valuable use of time when remediating an incident. We recommend that the criteria are reconsidered and that the incident should only be reported on the basis of reputation when the firm has been unable to provide adequate services. An incident that is subject to social media speculation or is reported within local news could represent a low impact incident whereas the criteria includes the firm losing clients or counterparts with a “material impact on its business.”
* The inclusion of case studies within the CP, while clarifying the intent of the FCA to receive incidents, results in discrepancy regarding the criticality of incidents vis-a-via the PRA. This includes an example whereby an incident could have an impact on ‘some’ clients that introduces an impact to any aspect of ‘day-to-day management’ or a website being taken offline for an undetermined period without consideration of alternative banking services being provided by an app, Post Office or via phone. There is, in addition, a significant criticality difference between the outage of an entire digital bank’s IT infrastructure in case study 8 versus case study 5 with a website being offline. We are concerned that the ‘consumer harm’ criteria has been interpreted widely and has become disconnected from the resilience regime where it has already been defined and connected to Important Business Services.
* The PRA includes the internal classification and processes of the firm as a standalone criteria within their assessment thresholds whereas the FCA does not. We recommend the FCA includes internal classifications as a specific criteria to align with the PRA. A firm’s internal classifications align with the existing UK operational resilience regime and the thresholds of each regulator. Classifications will include a firm’s thresholds to determine severity of impact, which will be directly related to the other assessment criteria proposed by the FCA (e.g. ability to provide services, impact on the firm’s clients and data loss). Ensuring the regime is as connected as possible to a firm’s internal incident management process should be a key priority of both the PRA and FCA.

We have certain concerns regarding the case studies used by the FCA and the reduction in thresholds implied by the examples utilised. We would consider the following amendments or removals:

* Case study 1: The case study includes the failure of processing of client interactions, IT system failure and banking access removal. A case study more reflective of a firm’s internal classifications could refer to the services as Important Business Services, mention a breach of threshold when a certain number of consumers were affected and a reference back to the FCA’s market integrity and consumer harm threshold.
* Case study 2: The case study should reference that the incident did not cause intolerable harm and did not result in incident remediation activities that were above business-as-usual within internal processes.
* Case study 3: We do not believe the incident described in the case study is realistic. The impact to payments should be reported by the supplier under the inability to provide adequate services. A firm should not be anticipated to predict the actions of other firms.
* Case study 4: We believe this case study is overly complex. The failure should relate to the inability to provide services or direct impact on customers. It is unclear why the FCA would require reports from E and F that would have been provided with more tangible information by firm G.
* Case study 5: The example provided could be demonstrating an effective substitution of services with minimal to no customer impact. The DDoS attack example disrupting the ability to provide services should cause firm safety and soundness alongside consumer harm, but the addition of effective substitution and a lack of clear consumer impact obfuscates the example.
* Case study 7: This case study is overly complex and includes complex topics such as reconnection (and sector-based response), IT system disruption, manual upload, concentration risk and impact on competitor platforms. The example, in addition, would reflect a market-wide impact with high levels of supervisory intervention. Effective substitution and consumer impact elements are missing from the case study. A firm is highly likely to have informed the FCA via Fundamental Rule 7.
* Case study 8: The case study includes an extensive outage and vast consumer impact across banking services, apps and transactions and, for some reason, is justified as requiring a report on the basis of a reputational risk due to utilising a cloud provider. We recommend this case study is reconsidered and reputational risk is more appropriately focused.
* Case study 9: The regulatory obligation requirement could relate to a missed tax filing or delaying an RFI response. These aspects are where proportionality and clarity is required.

**Q4: Do you agree with the proposed approach to standardise the formats of incident reporting?**

A standardised approach to reporting is helpful, as having one single reporting format results in operational consistency for firms and allows for more efficient incident management. The lack of standardised approach to the assessment criteria, on the other hand, results in incident triages requiring assessment across both the FCA and PRA, thus reducing the benefit of one format.

We would like to share our feedback relating to both the number of and timing of the reports:

* The initial report includes required fields that would require review and sign off prior to submission by the same individuals involved in addressing the operational disruption.  This is a potential distraction to dealing with the issue at a critical point.
* The initial report includes a field on the presumed root cause of the incident. Opining on the root cause within the first few hours of a major incident for the purpose of completing a regulatory notification may hinder resolution efforts as this assessment can only practically be made by the incident management team.
* If retaining Principle reporting, firms should have the capability to report in one format only (the one proposed in the CP). Firms should not be expected to report twice in relation to the same incident.
* We believe that the intermediate report criteria should be only when the firm believes that is further information that is relevant to regulators/supervisors in relation to the incident. Examples should be when the materiality of the incident has increased, a further threshold has been met or a further regulator needs to be notified of the incident. The criteria included for ‘significant change’ to determine whether an intermediate report is required are too prescriptive and denote minimal changes to the incident. This will likely result in multiple intermediate reports for each incident due to non-essential changes. The factors provided have limited recognition of how information is gathered and how the impact of an incident is quantified. This is a gradual process with continual refinement as an incident is remediated and/or isolated. Greater proportionality should be applied with greater levels of firm discretion, otherwise we are concerned there will be multiple unnecessary intermediate reports. The following criteria are too minimal to require an extra reporting phase:
	+ When additional information is available that provides more context on the incident.
	+ When the known impact of an incident changes.
	+ When the firm has taken action to mitigate the impact of the incident.
	+ Whether any mitigation action has been successful or not.

**Q5: 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?**

Please refer to our response to question 4.  There is a risk that the requirements of the initial report might distract from the need to investigate and respond to the incident.

The intermediate reporting criteria is the period whereby a strict interpretation of the requirements would result in material overreporting. We recognise the intent is to be proportionate in this phase, but further proportionality should be included within the proposal for this to be realised.

Please also refer to our response to question 3. As currently drafted, the proposed reporting threshold will, in our view, lead to excessive reporting of ‘low’ severity incidents, incurring considerable expenditure of time and resources at firms, and for little benefit. We argue this phase could also result in firms being expected to undertake subjective analysis of wider impact, which will have limited connected to the individual incident in question. We do not consider this information as useful to any regulator deciding whether to intervene and therefore do not consider this to be the collection of the ‘right information’.

Regulated firms are often subject to considerable supervisory requests when an incident is reported. Further clarity should be provided outlining how the FCA will respond to initial, intermediate and final reports. Greater consistency in information requests will allow firms to anticipate requests and provide more useful information. The greatest benefit to firms would be the recognition from supervisory teams regarding the FTE required to response to RFIs during an incident. Guidance to incident management and supervisory teams regarding consistent information requests and normalised timelines would greatly aid firms and would allow remediation to occur more efficiently.

The EU’s Digital Operational Resilience Act (DORA) removed data fields that required firms to comment on legal or regulatory non-compliance. The financial sector has reflected similar concerns to the FSB’s FIRE consultation. A firm is unlikely to provide detailed information relating to legal or regulatory non-compliance within a report where the receivers of that report are unknown. This should not be the basis for operational incident reporting criteria and firms should not be expected to hypothecate on legal exposure within reporting.

We would appreciate more detail on the level of resource the FCA will dedicate to analysing the information it will receive.

We are also interested in understanding how the FCA expects incident reporting requirements would play out in system-wide scenarios, such as the recent CrowdStrike incident. As far as we understand, significant high-profile incidents, such as CrowdStrike type events, are not the motivation behind the proposals. Had these proposals been in place during the recent CrowdStrike incident, it is likely the FCA would have received potentially thousands of similar incident reports all at once. It is difficult to see how the FCA would be able to usefully digest this information. The aggregate effort on the part of firms to complete incident reports would, on the other hand, be significant effort diverted away from handling the incident itself. In such circumstances, it may be helpful for the FCA have a mechanism to signal to firms that it is aware of the incident and that it does not require further incident reporting (e.g. interim reports) relating to the issue.

**Q6: Do you agree with the proposed definition of third party arrangements?**

The inclusion of c), i.e. defining companies within a group structure as third party arrangements, doesn’t necessarily address the global nature of firms that are functionally organised. We therefore suggest removing c) from the definition.

**Q7: Do you agree with the proposed definition of material third party arrangements?**

We suggest using more precise language than ‘could’ in the definition to ensure that the definition is interpreted proportionately. For example, by replacing ‘could’ with ‘likely to’.

We recommend adding a time element to the ‘cause intolerable levels of harm to the firm’s clients’ criteria, i.e., ‘cause intolerable levels of harm to the firm’s clients **within a reasonable amount of time**’.

We also suggest aligning the definition of material third party arrangements to those arrangement supporting Important Business Services.

The CP states that the material third-party reporting requirements would only apply to a sub-set of firms whose services, if disrupted, could have significant consumer or market impact. Within this sub-set the FCA has included Enhanced SM&CR firms. We would encourage the FCA to review its proposal to include Enhanced SM&CR firms in this sub-set as not all are categorised as an entity which may cause significant harm. For example, some Enhanced SM&CR firms are not relationship managed due to their assessed level of risk by the FCA. As such we would recommend focusing on only those firms which would more likely be relationship managed due to the significant impact on consumers and markets if disrupted.

A further important point is that currently the SM&CR regime is under review by the FCA and so there is a risk to firms which are categorised as Enhanced of building out processes and procedures on a regime which may be subject to significant change.

**Q8: Do you have any comments on our proposed notification requirements including the impact on the number of arrangements that will be reported?**

Please see our response to question 6. We would suggest removing c) from the proposed definition of third party arrangements.

**Q9: Do you think the mechanism to submit and update the structured register of firms’ material third party arrangements is proportionate?**

We do not have any comments on this question.

**Q10: Do you have any comment on the template which includes the information on third party arrangements to be shared with us?**

Many of the firms in scope of these proposals have recently undertaken considerable effort preparing their registers of information for DORA. As far as possible, the FCA’s template should be compatible with the DORA register of information template, so that firms are able to leverage the work they have already done, rather than have to revisit all of their third party providers again.