FCA Policy Statement on operational resilience

FCA Policy Statement on operational incident and third party reporting

On 18 March 2026, the Financial Conduct Authority (FCA) published its Policy Statement (PS26/2), introducing final rules and guidance on operational incident reporting and material third-party arrangement reporting. These rules represent a significant overhaul of how regulated firms must report operational disruptions and manage their third-party relationships, establishing a single, coordinated regime across the FCA, the Prudential Regulation Authority (PRA) and the Bank of England (BoE).

For **operational incident reporting**, the FCA has introduced a two-tier framework comprising '*standard*' reporting for approximately 90% of FCA solo-regulated firms and '*enhanced*' reporting for a smaller subset of strategically important firms. Standard reporting requires completion of a single short form with only 10 mandatory questions, representing a significant reduction from the original consultation proposals. Enhanced reporting maintains a three-phase structure but consolidates this into a single dynamic form with approximately 20% fewer questions overall.

For **third-party reporting**, the sub-set of firms within scope must notify the FCA of new material third-party arrangements and significant changes to existing arrangements, and must submit an annual register of all material third-party arrangements. Third-country branches have been excluded from notification requirements but remain subject to the annual register submission.

The new framework will come into force on **18 March 2027**, giving firms twelve months to prepare for compliance.

Background and rationale

The regulators have emphasised that operational incidents can disrupt firms' services, harm consumers, affect market confidence and disrupt the UK financial system. Feedback prior to consultation indicated that many firms were unclear on when and how to report operational incidents, what incidents should be reported, and what information was required.

In 2025, over 40% of cyber incidents reported to the FCA involved a third party, underscoring the systemic risks posed by third-party dependencies. The new framework is designed to provide the regulators with timely, accurate and consistently structured data to help them better understand the interconnectedness of the industry, triage incidents, identify sector-wide stresses, and understand concentration risks.

The regulators have sought to align the regime, where appropriate, with international frameworks including the EU's Digital Operational Resilience Act (DORA) and the Financial Stability Board's Format for Incident Reporting Exchange (FIRE).

Scope of the new rules

Operational incident reporting

The final rules on operational incident reporting apply to a broad population of regulated entities. The following are within scope:

- All firms with a Part 4A permission;
- Payment service providers (PSPs);
- UK recognised investment exchanges (UK REIs);
- Registered trade repositories; and
- Registered credit rating agencies.

The FCA has deliberately retained all firms within the scope of incident reporting, noting that experience has shown that the impact of incidents can be felt across the sector and is not limited to larger firms. However, the level of reporting required differs depending on the firm category.

The '***enhanced reporting***' requirements apply to:

- Enhanced scope SMCR firms;
- Banks;
- Designated investment firms;
- Building societies;
- Solvency II firms;
- CASS large firms;
- PSPs;
- UK RIEs; registered trade repositories; and,
- Registered credit rating agencies.

All other firms with a Part 4A permission fall within the '***standard reporting***' category, which represents approximately 90% of the FCA-regulated firm population.

Third-party reporting

The third-party reporting requirements apply to the following, more limited, subset of firms:

- Enhanced scope SMCR firms;
- Banks;
- Designated investment firms;
- Building societies;
- Solvency II firms;
- CASS large firms;
- UK RIEs;
- Authorised electronic money institutions and authorised payment institutions; and
- Consolidated tape providers.

Third-country branches remain in scope of the annual register requirement, reflecting that many significant firms operate as branches in the UK and the FCA requires visibility of their third-party dependencies since, if disrupted, these could have a significant impact on the UK financial system. However, third-country branches have been excluded from the notification requirements for new or changed material third-party arrangements.

Key definitions

Definition of an operational incident

The FCA and PRA have adopted a single, harmonised definition of an '*operational incident*'. An operational incident is defined as:

> *"Either a single event or a series of linked events which disrupts the firm's operations such that it:*
>
> *(a) disrupts the delivery of a service to an end user external to the firm; or*
>
> *(b) impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to such an end user."*

A '*series of linked events'* includes events with a cumulative impact that disrupts a firm's operations, including connected events sharing the same root cause or an incident beginning with a third-party failure causing downstream impacts.

Importantly, '*end users external to the firm*' include retail customers, business customers, market participants, other legal entities, trustees, supervisory regulators and members of the firm's group. Firms do not need to report 'near misses', that is, potential incidents that were thwarted or crystallised incidents that were contained before meeting any reporting threshold. Planned, controlled interruptions (such as routine system updates) are not reportable unless they fail and result in disruption meeting a threshold.

Third-party arrangement

A '*third-party arrangement*' is defined as an arrangement of any form between a firm and a person who provides a product or service to the firm, whether or not the product or service is:

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

The definition uses the term '*person*', which is a defined FCA Handbook term that includes corporate or unincorporated bodies and encompasses all types of entities. The FCA has rejected suggestions to limit the definition to arrangements provided on a '*recurrent or ongoing basis'*, noting that firms must decide whether a product or service is material based on the risk it poses, regardless of whether it is provided on an ongoing or one-off basis.

Material third-party arrangement

A '*material third-party arrangement*' is defined as a third-party arrangement which is of such importance that a disruption or failure in the performance of the product or service provided to the firm could:

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

Firms are responsible for assessing the materiality of their third-party arrangements on a case-by-case basis and should develop their own processes for assessing materiality as part of their third-party risk management policy. The FCA has declined to introduce monetary thresholds to define materiality, noting that such quantitative thresholds would need to apply to firms of vastly differing scale and nature and would be unduly complicated and prescriptive.

The FCA has not limited the definition of materiality to third-party arrangements affecting an important business service, noting that even arrangements not directly linked to an important business service could have a significant impact if disrupted.

1. Operational incident reporting framework

Reporting thresholds

A firm must report an operational incident where it **reasonably believes** the incident poses a risk:

- **Consumer harm**: of causing intolerable levels of harm to consumers from which consumers cannot easily recover;
- **Safety and soundness**: to the safety and soundness of the firm and/or other market participants; or
- **Market stability**: to market stability, market integrity or confidence in the UK financial system.

The concept of '*reasonable belief*' has been incorporated into the threshold test. This reflects that the FCA expects firms to use their judgement and act in a reasonable way based on the circumstances and available information. The regulators have deliberately avoided prescriptive quantitative thresholds, given the wide variation in scale and nature of firms in scope. Firms may use their own internal risk frameworks to assist in triaging incidents, provided those frameworks are consistent with the regulatory thresholds.

Not all thresholds will be equally relevant to all firms. For example, if a firm does not have direct consumer relationships, it may be less likely to meet the consumer harm threshold, and similarly some firms would be much less likely to experience an incident that could threaten the UK financial system.

Two-tier reporting structure

A key change is the introduction of a two-tier reporting structure:

Standard Reporting

Standard reporting applies to approximately 90% of FCA solo-regulated firms and requires submission of a single short form with a small number of questions. Firms do not have to update this report after submission, although they may need to contact the FCA under general notification requirements in accordance with Principle 11 if further information about an operational incident emerges.

The standard report requires 10 mandatory fields, including:

- Status of the incident;
- Trigger for reporting;
- Type of incident;
- Incident title;
- Description;
- Firm severity rating;
- Time of detection;
- Actions planned to recover;
- Actions taken to recover; and
- Time of resolution if resolved.

Enhanced Reporting

A smaller cohort of firms listed in SUP 15.18.3R are required to submit '*enhanced*' reports. This report requires more information than the standard reporting form but less than the forms originally consulted upon, with the number of questions reduced overall by approximately 20%, with much of this reduction at the initial phase.

Although the FCA has moved to a single form, it has maintained the three-phase process comprising initial, intermediate and final phases. Firms update this form to provide significant updates if necessary, including to indicate that an incident has been resolved.

For the **initial phase**, enhanced reporting firms must submit information including:

- Authority receiving the report;
- Status of the incident;
- Trigger for reporting;
- Type of incident;
- Incident title;
- Description;
- Firm severity rating;
- Time of detection; and
- Actions planned and taken to recover.

For the **intermediate phase**, firms must submit additional information as soon as practicable after any significant change in circumstances, including information on:

- Discovery method;
- Business services affected;
- Service disruption type;
- Level of geographic spread; and
- Origin of the incident.

For the **final phase**, firms must submit additional information including:

- Time of resolution;
- Service downtime;
- Number and percentage of affected customers;
- Value and number of transactions affected;
- Affected party types;
- Cause type;
- Type and properties of resource affected;
- Lessons identified; and
- Remedial actions being taken.

Reporting timelines

All firms must submit reports **as soon as practicable** after determining that an incident meets a threshold. The FCA expects this to be within **24 hours** at most of making that determination.

PSPs must continue to report within **4 hours** of first detecting a major operational or security incident, reflecting the time-sensitive nature of incidents in the payments sector.

Enhanced reporting firms must provide material updates during the intermediate phase if there are significant changes to an incident's status. A final report must be submitted within **30 working days** of the incident being resolved, or in exceptional circumstances, within **60 working days**.

Given the tight timeframe for reporting, we would recommend that firms familiarise themselves with the FCA's Guidance and the types of incidents that are likely to be reportable, in order to minimise the need to conduct lengthy analysis in time sensitive, high pressured situations.

Submission platform

All incident reports must be submitted via the FCA's **Connect platform**. Dual-regulated firms will make a single submission that is automatically shared with the PRA. This represents a significant simplification from the previous arrangements. The Connect platform recognises submissions at the **entity level**, not the group level, meaning firms must submit an incident report for each firm in a group that is experiencing an incident which meets the reporting thresholds.

Only **one report per incident** is required, even where multiple services are affected; firms can list multiple affected services in the relevant field in the reporting form.

Subsuming existing regimes

The new framework subsumes existing incident reporting regimes for PSPs (previously under the EBA Guidelines on incident reporting under PSD2) and registered Credit rating agencies (CRAs) (previously under ESMA reporting guidelines). From **18 March 2027**, these firms will report under the single framework set out in SUP 15.18.

2. Third-party reporting framework

Scope

The third-party reporting requirements apply to a more targeted group of firms:

- Enhanced scope SM&CR firms;
- Banks;
- Designated investment firms;
- Building societies;
- Solvency II firms;
- CASS large firms;
- UK RIEs;
- Authorised e-money institutions and payment institutions; and
- Consolidated tape providers.

Third-country branches are excluded from the notification requirements but remain in scope for the annual register submission.

Notification requirements

Firms within scope must notify the FCA when **entering into, or significantly changing**, a material third-party arrangement. A '*significant change*' is one that materially alters the nature, scale or complexity of the risks inherent in the arrangement, such as:

- A material increase or decrease in the scope of services provided;
- A change in how the third party stores, processes or accesses sensitive data;
- Moving data storage to a new location;
- A material change to the ownership or financial position of the third party; or
- A change in third party or key sub-contractor.

The FCA expects firms to notify the regulator at an **early stage** and to submit the notification before making any internal or external commitments. Notification should be made sufficiently early in the firm's decision-making process to allow for any engagement that the FCA may consider appropriate, before the firm becomes contractually or operationally committed. However, the

notification process is not an approval mechanism; while the data will inform thematic and industry-wide analysis, the FCA may not respond to every submission.

Firms are not required to resubmit the register each time a notification is required; the register is submitted on an annual basis and only once the FCA notifies firms that the submission window is open.

Annual register

Firms within scope must **maintain a register** of their material third-party arrangements and **submit it annually** to the FCA. The annual submission will be made via FCA RegData within 90 calendar days of the submission window opening.

The register data, together with notification data, will assist the regulators in understanding systemic third-party risk and help identify potential critical third parties (CTPs) for recommendation to HM Treasury.

The regulators have retained the **supply chain ranking requirements**. Firms are increasingly using third parties to support important business services, and many of these arrangements rely on multiple service providers. The supply chain ranking allows the regulators to identify critical nodes in a firm's supply chain with more accuracy.

Legal Entity Identifier (LEI) has been retained as the unique third-party identifier, with a '*not applicable*' option added for third parties that do not have an LEI.

Intragroup arrangements

For most firms, intragroup arrangements (or, for ring-fenced bodies, arrangements where the provider is a '*permitted supplier*') need only be reported where there is an **external third-party dependency**.

The exception is UK RIEs, which **must report all material intragroup arrangements** given the integral nature of such arrangements to their operations.

Implications for different firm types

Banks and dual-regulated Firms

For banks and other dual-regulated firms, the new framework represents a significant simplification. Rather than navigating separate FCA and PRA regimes, these firms will benefit from:

- **Single definitions**: A harmonised definition of '*operational incident*' and '*material third-party arrangement*' across both regulators.
- **Single submission portal**: One report via FCA Connect that is automatically shared with the PRA.
- **Unified templates**: Identical reporting templates for incidents and third-party arrangements.

Dual-regulated firms should note that each regulator's thresholds remain linked to its respective statutory objectives. An incident may meet the thresholds of one regulator, both regulators, or initially meet one and subsequently meet the other as the incident evolves. Firms should select the relevant regulator(s) in their incident report and update as necessary.

Banks fall within the scope of **enhanced incident reporting**, requiring submission of phased reports (initial, intermediate, final) with more detailed information. They are also in scope for material third-party notification and annual register requirements.

Solo-regulated firms (standard reporting)

The overwhelming majority of FCA solo-regulated firms will be subject to **standard incident reporting**.

This represents a significantly reduced burden compared to the consultation proposals and should enable smaller firms to comply with the framework without disproportionate cost or complexity.

Solo-regulated firms that are not enhanced scope SM&CR firms, designated investment firms, Solvency II firms or CASS large firms will **not** be in scope for the third-party notification and register requirements.

Enhanced scope SM&CR Firms

Enhanced scope SM&CR firms are subject to the full suite of requirements under both policies:

- **Enhanced incident reporting**: Three-phase reporting with more detailed information requirements.
- **Third-party notifications**: Obligation to notify the FCA when entering into or significantly changing material third-party arrangements.
- **Annual register**: Requirement to maintain and annually submit a register of material third-party arrangements.

These firms should expect greater regulatory scrutiny of their operational resilience and third-party risk management arrangements.

Payment service providers (PSPs)

PSPs will see their existing incident reporting obligations under the EBA Guidelines disapplied and replaced by the new framework. Key points for PSPs include:

- They fall within enhanced incident reporting but retain their existing 4-hour reporting deadline (measured from first detection) for the initial report phase.
- Reports submitted under the new framework will also satisfy the notification requirement under Regulation 99(1) of the Payment Services Regulations 2017.
- Authorised payment institutions and authorised e-money institutions are in scope for third-party notification and register requirements.

The guidance includes specific factors for PSPs to consider when assessing whether an incident meets the notification thresholds, reflecting the time-sensitive nature of disruption in the payments sector.

Implementation timeline and next steps

The new rules come into force on **18 March 2027**, providing firms with 12 months to prepare for compliance. During this period, the FCA will engage with firms to support them in adapting to the rules and reporting technologies. Two years after implementation, the FCA will review the policies to assess if they meet both the regulator's needs and those of firms.

The FCA has published accompanying Finalised Guidance documents: FG26/3 on Operational Incident Reporting and FG26/4 on Material Third Party Reporting. Firms should read these guidance documents alongside the rules.

Firms affected by these changes should consider the following preparatory steps during the 12-month implementation period:

1. **Review existing incident response frameworks**: Assess whether current internal incident classification and escalation procedures are consistent with the new regulatory thresholds.

2. **Identify the applicable reporting tier**: Determine whether the firm falls within standard or enhanced incident reporting, and whether it is in scope for third-party notification and register requirements.

3. **Map material third-party arrangements**: Conduct a comprehensive review of third-party arrangements to identify those that meet the definition of '*material third-party arrangement*'.

4. **Establish governance arrangements**: Ensure clear accountability and responsibility for meeting the new requirements, including appropriate senior management oversight of material third-party arrangements.

5. **Prepare for register submission**: Build or adapt internal systems to maintain the required register information in the standardised format.

6. **Train relevant personnel**: Ensure staff responsible for incident management and third-party oversight understand the new requirements, thresholds and reporting processes.

7. **Engage with FCA Connect**: Familiarise relevant personnel with the FCA's Connect platform through which all incident reports and third-party notifications must be submitted.

The new operational incident and material third-party reporting framework represents a significant step towards a more unified and coherent approach to operational incident and third-party reporting across the UK financial services sector. The creation of single regimes across the FCA, PRA and the BoE, together with the reduction in information requirements for the majority of firms, should help to reduce regulatory burden whilst still ensuring the regulators receive the data they need to supervise firms effectively and identify systemic risks.

The policy statement makes clear that operational resilience remains a supervisory priority for the FCA. The data collected under both the incident reporting and third-party reporting frameworks will be used to identify risks, enable timely regulatory interventions, and in the medium to long term, to develop thematic insights to share with industry to improve practices.

Firms should begin their implementation planning promptly to ensure they are well-positioned to comply with the new requirements when they come into force in March 2027.