Finalised Guidance

Operational Incident Reporting

FG26/3

March 2026

Contents

1 Introduction

1.1 This Finalised Guidance sets out our expectations of how firms should comply with our requirements to report operational incidents.

1.2 We expect firms to establish clear accountability and responsibility for meeting these requirements.

1.3 This guidance covers:

- The meaning of 'operational incident'.
- Operational incident thresholds.
- Our overall approach to incident reporting.
- How to complete an incident report (standard and enhanced reports).

1.4 This guidance is relevant to:

Standard reporting firms:

- all firms with a Part 4A permission (except enhanced reporting firms).

Enhanced reporting firms:

- Enhanced scope SMCR firms
- Banks
- Designated investment firms
- Building societies
- Solvency II firms
- CASS large firms
- Payment service providers
- UK RIEs
- Registered trade repositories
- Registered credit rating agencies

1.5 This guidance should be read in conjunction with:

- Policy Statement: Operational Incident and Material Third Party Reporting (PS26/2); and
- FCA handbook SUP 15.18.
- For dual regulated firms only, PRA Supervisory Statement SS1/26

2 Background

2.1 Operational incidents can disrupt firms' services, which in turn can harm consumers, affect market confidence and disrupt the UK financial system. We need to receive information on significant incidents in a timely and structured way to quickly understand the impact, what a firm is doing to resolve the problem and to decide if we need to take steps in response.

2.2 Before publishing CP24/28, industry told us some firms were unclear on when and how to tell us about operational incidents. Some firms were unclear which incidents they should tell us about and what information we needed.

2.3 PS26/2 introduced new rules giving firms a standardised process for reporting relevant operational incidents. The rules define an operational incident and set out the thresholds for firms to assess which incidents to report. We have divided firms into 2 groups for reporting incidents: 'standard' and 'enhanced'. This is because we may need more information from some kinds of firms when they have serious incidents.

2.4 Most firms will have a simplified 'standard' reporting process as set out in Chapters 5 and 6. A subset of firms have an 'enhanced' reporting process as set out in Chapters 5 and 7.

2.5 The reports we receive will help us to triage operational incidents and to respond where necessary. These reports will also help us to carry out broader thematic analysis, which will help us to provide insights to industry.

2.6 This guidance is to help firms assess whether an incident meets our definition of an operational incident, and if it is reportable under our rules. It also clarifies what firms should do if they need to report, and when to do it.

Payment service providers and registered credit rating agencies

2.7 The separate incident reporting frameworks for Payment Services Providers (PSPs) and registered Credit Rating Agencies (CRAs) will both be replaced by the one in this document from 18 March 2027. There are provisions specific to PSPs in the Handbook, as set out in PS26/2.

Firms regulated by the FCA and the PRA (dual regulated firms)

2.8 As the FCA and PRA have a single reporting regime for incidents, we set out how dual regulated firms should consider the thresholds of both regulators.

3 Definition of 'operational incident'

3.1 This chapter gives firms guidance to help assess whether an event meets our definition of an operational incident. We break down the definition of an operational incident and provide guidance and examples of how firms should interpret the following components of this definition:

- Linked events.
- An end user external to the firm.

3.2 This chapter also sets out guidance and examples on the types of incidents that may affect a firm's operations and services. Under these rules, firms only need to report an operational incident that has crystallised and met one or more of the FCA's thresholds. In practice, these are incidents which have a significant impact on our objectives.

3.3 In the Handbook Glossary we define an operational incident 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.'

Linked events

3.4 A 'a series of linked events' includes events with a cumulative impact that disrupts a firm's operations. This may include connected events, often sharing the same root cause. This could be an incident beginning with a third party failure causing downstream impacts. Or this could be multiple disruptions triggered by the same issue.

3.5 To help explain this concept, we give some examples below of a 'series of linked events'. This is not a full list and, as always, firms should consider their specific circumstances.

- A third party cloud service provider's data centre suffers an outage due to a pre-existing technical fault. This causes a firm's banking and payments platform hosted by the cloud service provider to go offline. The bank is unable to fail over to another vendor to resume provision of services. The firm's end users cannot use digital applications, view their balances, or make payments.

  The linked events are the: technical fault at the third party; the firm's failure to fail over to another vendor.

- A technology analyst uploads an incorrect payment configuration file during end of day processing. This results in the end of day reconciliation failing to flag mismatched transactions. The reconciliation failure leads to the firm issuing incorrect settlement instructions, resulting in the failure or delay of a high volume of transactions and misallocation of funds across a considerable number of end users. The firm unwinds the transactions manually, resulting in further extended disruption to end users' access to their funds.

The linked events are the: configuration error; reconciliation control failure; incorrect settlement instructions.

End users external to the firm

3.6 When determining whether an event constitutes an operational incident, a firm must assess whether the event affects an end user external to the firm. These end users should be identifiable and may include consumers, business customers, market participants, other legal entities, trustees, supervisory authorities or members of its group.

Interaction with other systems for assessing impact

3.7 Firms must assess whether an incident meets the definition of an operational incident, whether or not this affects the delivery of an important business service (IBS), or data associated with one. This is because an operational incident may originate from a resource not attributed to an IBS and still pose a risk that meets our thresholds. While all FCA firms are subject to either our standard or enhanced incident reporting rules, the concept of impact tolerances (ITOLs) and IBSs is not relevant to all of these firms. Where relevant to a firm, we would expect it to report an incident before ITOLs are breached.

These examples show how an incident not affecting an IBS can be reportable under this framework:

- A cyber-attack, such as a malware or ransomware attack, targets a customer portal and results in unauthorised access and compromise of sensitive data belonging to external end users. The incident generates significant negative media coverage, such that it could have severe reputational effects on the firm and cause loss of confidence among financial counterparties or customers to deteriorate, leading them to exit relationships with the firm and risking its safety and soundness.

  Data loss incidents may not affect an important business service. However, under the policy we would expect a firm to report this incident. This is because the data could be used to cause harm to those users, for example, by cyber threat actors or by market participants taking advantage of commercial data.

- An IT failure affecting a firm's payment routing system results in an inability of the firm to complete or process a high number of transactions. The incident leaves the firm unable to deliver multiple business services which the firm has not classified as important business services, resulting in its failure to meet contractual obligations and therefore risk its safety and soundness.

  Outages in seemingly low-impact or non-critical services can rapidly escalate through a cascade effect, where failures in small, interconnected components create widespread operational disruption. Such incidents can hinder a firm's ability to meet contractual obligations, negatively affect customers and counterparties, and ultimately pose risks to the firm's safety and soundness.

3.8 It is up to firms to implement a framework for assessing whether an incident has met one of our thresholds. We have not aligned the definition of 'operational incident' to the concept of IBSs. However, a firm may choose to refer to the IBSs they monitor when assessing incidents, as well as adopting pre-existing internal risk assessment and crisis response frameworks.

Near misses

3.9 Under SUP 15.18, firms only need to report an operational incident that has crystallised and met one or more of our thresholds. In practice, firms should report incidents with a significant impact on our objectives. So firms do not need use the processes set out in SUP 15.18 and in this document to report 'near misses' such as:

- a potential incident that was thwarted (eg an unsuccessful distributed denial of service (DDOS) attack), or
- a crystallised incident that was prevented or otherwise contained and did not meet one or more of the thresholds in SUP 15.18.6R(1).

3.10 However, a firm should consider whether it should notify us of such an event under the general notification requirements in SUP 15.3.1R and Principle 11, where applicable. The general notification requirements include disclosing to us anything relating to the firm which we would reasonably expect notice of (Principle 11). It also includes notifying us of matters with a serious regulatory impact (SUP 15.3.1R). Such notifications should be made through the firm's usual supervisory channel, rather than through the SUP 15.18 incident reporting mechanism.

Planned interruptions

3.11 An operational incident does not include a temporary, controlled interruption to a service. For example, one resulting from a planned systems update or routine change which goes to plan. However, if such a controlled interruption does not go to plan and the firm is unable to return to provide services as expected, leading to one or more of the thresholds in SUP 15.18.6R(1) being met, the firm should report the incident. The following example illustrates this type of an operational incident:

- A scheduled IT upgrade fails and results in a technology outage which disrupts access to a retail bank's mobile banking application. The bank reasonably believes the incident could cause intolerable harm to consumers, as it disrupts access to a service that helps consumers navigate their financial lives and so meets the FCA's consumer harm threshold.

  As the IT upgrade has resulted in disruption that meets a threshold, the firm must submit an incident report.

4 Thresholds and factors to consider

4.1 This chapter sets out the incident thresholds and examples of the factors we expect firms to consider when assessing if an incident meets the thresholds. We also give some examples of incidents that would meet the thresholds. This includes some case studies for Payment Service Providers (PSPs), which have additional sector-specific factors to consider.

Operational incident thresholds

4.2 The threshold for reporting under this framework is met where a firm reasonably believes an operational incident meets one or more of the notification thresholds – namely, that it poses a risk:

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

In this document, we refer to these as the consumer harm, safety and soundness and market stability thresholds respectively. See SUP 15.18.6R(1).

4.3 Firms also regulated by the PRA should also consider whether an incident meets the PRA's thresholds (see 7.15). The PRA also has a safety and soundness threshold. When reporting an incident that has met this threshold, a dual regulated firm will report to both regulators by submitting a single report.

Factors to consider

4.4 We expect firms to consider a range of factors when assessing whether an incident meets any of the thresholds for notifying us. For example:

- The direct impact on the end users or the wider sector, including its counterparties and other market participants.
- The reputation of the firm or the financial sector.
- The firm's ability to meet its legal and regulatory obligations.
- The firm's ability to provide adequate services.
- The firm's ability to safeguard the availability, authenticity, integrity or confidentiality of information or data of an end user external to the firm.
- The firm's internal assessment and classification of the incident.

4.5 These factors indicate the type of considerations we expect firms to make when assessing whether to report an operational incident. Firms should not use this as a 'tick box' list. Every firm's circumstances are unique and so we cannot provide a definitive list of factors. Firms may wish to consider other relevant factors such as their own internal incident risk frameworks and metrics specific to their business model when making this assessment, provided these frameworks are consistent with our thresholds.

Payment services providers (PSPs)

4.6 PSPs have specific factors to consider, because the fast and direct impact on consumers, including potentially vulnerable ones, make incidents in this sector especially time sensitive. When assessing whether an incident meets any of the thresholds in SUP 15.18.6R(1), we expect PSPs to consider the same kinds of factors in 4.4 above, as well as the following:

- Proportion of transactions affected.
- Proportion and nature of payment service users affected.
- Service downtime, and
- The impact on their distribution channels.

4.7 To help illustrate this, the following case studies give examples of some of the kinds of incidents we would expect a PSP to report under the process set out in SUP 15.18 and in this document:

- **Case study 1 – cyber incident**

  A PSP suffers a cyber incident resulting in users losing access to their accounts online. The incident lasts for more than 2 hours, affecting more than 10% of the PSP's normal number of payment transactions, totalling more than £100,000, and affecting over 10 per cent of its payment service users, over 5,000 in all.

  Based on the multiple impacts to the number of transactions and payment service users affected and service downtime, the PSP makes an incident report to us.

- **Case study 2 – change in software**

  PSPs X and Y both make software changes which result in payment service users being unable to make point of sale payments. More than 25% of PSP X's normal number of payment transactions are affected. More than £5,000,000 (but less than 25%) of PSP Y's payment transactions are affected.

  Given the large number of transactions affected, PSPs X and Y both make initial reports to us.

- **Case study 3 – third party supplier failure**

  PSPs X and Y suffer systems failures caused by the same third party supplier. More than 25% of PSP X's payment service users are unable to receive income payments. More than 50,000 (but less than 25%) of PSP Y's payment service users are similarly affected.

  In view of the large number of payment service users affected, PSPs X and Y both make initial reports to us.

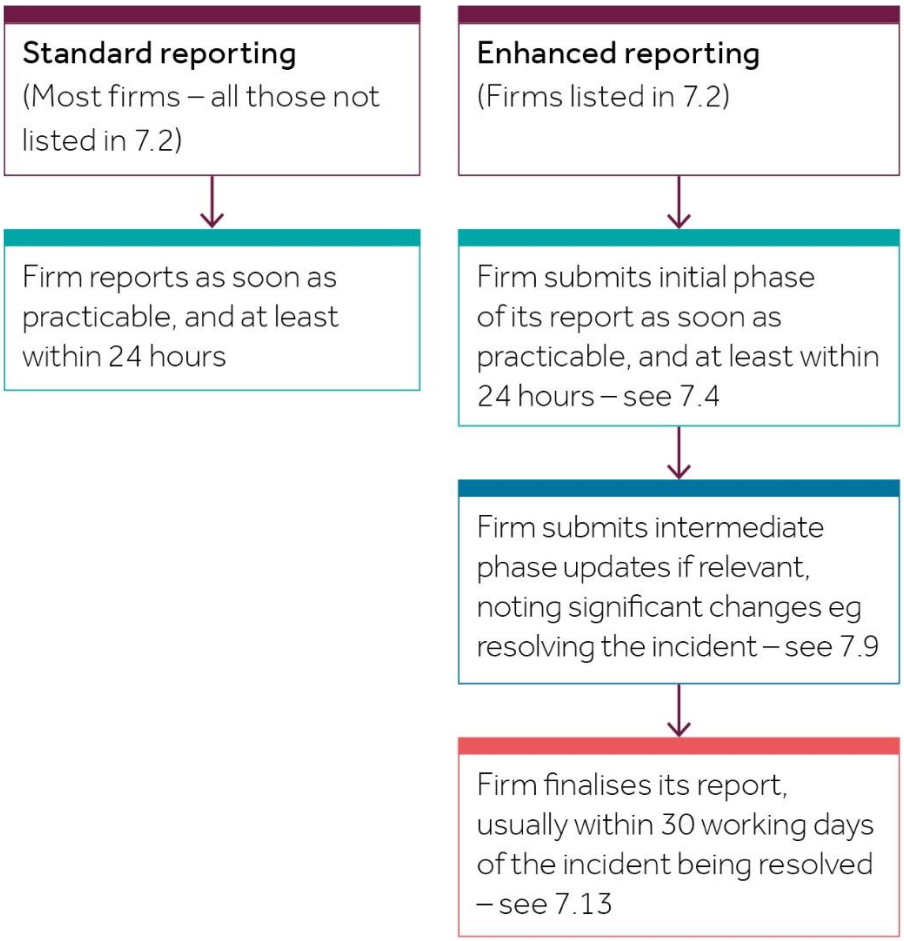
5 Overall approach to incident reporting

5.1 There are 2 tiers of incident reporting: 'standard' and 'enhanced'. Most firms must submit standard reports (see chapter 6). Only the subset of firms specified in SUP 15.18.3R (see chapter 7) must submit enhanced reports. A firm subject to standard reporting can choose to submit an enhanced report if it wants to provide more detail. Both standard and enhanced reports must be made in Connect.

5.2 Standard incident reporting is a single report requiring firms to provide basic information about an operational incident. In some cases, depending on the severity of the incident and quality of information submitted, we may request more information.

5.3 Enhanced incident reporting is more detailed, with firms reporting in 3 phases over the life cycle of an incident. These phases are 'initial', 'intermediate' and 'final'. Having made a report at the initial phase of an incident, enhanced reporting firms can return to the report to update it if there are significant changes to an incident's status. After the incident is resolved, firms finalise the report.

Figure 1: standard and enhanced reporting



5.4 We know that at the start of an incident most firms will be focusing on containing and resolving it. We have reduced the information requested at the initial stage to help firms focus on resolving incidents. Under enhanced reporting, not all questions are mandatory at each phase of the incident report, some information may be unavailable. However, where information is available, we expect firms to provide it.

5.5 While firms should report an incident within 24 hours of determining that it meets our thresholds, they should not wait 24 hours to report. In accordance with the rules, firms should do this as soon as practicable. PSPs should continue to report incidents within 4 hours of first detecting the incident, as this requirement has been kept in place from their previous reporting regime. We explain this further in Chapter 7.

6 Standard incident reporting

6.1 This chapter is for firms in scope of our standard incident reporting requirements. It provides guidance on how these firms should report to us if they have an operational incident that meets the thresholds in 4.2.

6.2 Standard reporting consists of a short report so firms can tell us about an operational incident. Table 1 sets out the field names and explains the information required in a standard report.

Note: enhanced reporting firms (those listed in SUP 15.18.3R) should instead see Chapter 7.

6.3 Unlike enhanced reporting, firms subject to standard reporting will not have to update their submission. Occasionally, we may engage further with a firm, depending on the quality of the information submitted, or the severity of the incident.

Reporting

6.4 Firms are not required to update a standard incident report once it has been submitted.

Required information

6.5 The table below is to help firms complete a standard incident notification in Connect. Please also see this detailed template.

Table 1 – standard reporting

Field name	Field Status	Description/Detail required
Status of the incident	Required	The firm must select the current status of an incident, including whether it is open, resolved, or closed. This is based on the FSB FIRE Taxonomy: - **Open:** the period between the time of detection and resolution. The firm/FMI is responding to the incident, minimising impact and prioritising recovery. - **Resolved:** the period between the time of resolution and closure. The immediate impact of the incident has been addressed, but the firm/FMI is still remedying vulnerabilities and conducting a post-incident review. - **Closed:** The post incident review has been conducted, outstanding vulnerabilities have been remedied and lessons learned have been identified.
Trigger for reporting the incident	Required	The firm must select the criteria that triggered the reporting of the operational incident. The firm must report to the FCA incidents that the firm assesses pose a risk to their objectives. This includes:

		- Consumer Harm (FCA) - Safety and Soundness (PRA/FCA) - Market Integrity (FCA)
Type of incident	Required	The firm must select the type of incident based on the definition of an operational incident as defined by the authorities. This includes: - **Disruption:** an operational incident that disrupts the delivery of a service to an end user external to the firm; - **Data loss:** an operational incident that impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to such end user.
Incident title	Required	The firm must add a brief headline to describe unique elements associated with the incident to facilitate reporting and engagement with the authorities. This is intended to be a short reflection of the incident, easy to access and interpret by a broad audience. The headline could evolve over time to reflect any changes in the firm's understanding of the incident.
Description of the incident	Required	The firm must provide any additional details that help describe the incident, including qualitative information on its nature and actions taken or planned for response and recovery, where these are not covered elsewhere in the form. They may also include indicative or confirmed root cause information, with any qualitative description not already captured in other sections.
Firm severity rating	Required	The firm must make an assessment of the severity rating of the incident based on its urgency and impact. The firm should make this assessment based on its own internal severity rating and incident categorisation, and should use the authorities' reporting criteria based on the FSB FIRE Taxonomy. The severity ratings include: - **Low:** Escalated within relevant functional units. Operational response (eg SOC, operations, technology) is sufficient. - **Medium:** Escalated to invocation of crisis management arrangements. - **High:** Escalated to the most senior level of crisis management command. The firm is activating its most senior command structure.
Time of the detection	Required	The firm must confirm the time at which the incident has been detected.
Actions planned to recover	Required	The firm must provide an overview of the planned incident response and recovery strategy, actions planned to mitigate the impact of an incident, and if available estimated timelines for resolution.
Actions taken to recover	Required	The firm must provide a brief overview of the response or recovery actions already taken to resolve the incident. The firm must consider adding any relevant information on the technical response or any key decisions taken at a tactical or strategic level.

Estimated time to resolve the incident	Optional if the incident is not resolved or closed	The firm may provide an estimated timeframe for incident resolution. The firm may provide an indicative timeline and indicate the level of confidence in the assessment under the actions taken or planned to recover.
Time of the resolution	Required if the incident is resolved or closed	The firm must specify the time at which the impacts associated with incident are brought under control and affected services restored to acceptable levels.
Cause type	Optional	The firm may select the root cause of the incident. The firm may provide an indicative root cause of the operational incident.
Origin of the incident	Optional	The firm may select a high level categorisation of the incident origin. This should include whose or what actions cause or contributed to the operational incident. o **Internal:** A firm resource employed directly by the firm. o **External**: A resource with no relationships with the firm. o **Third Party:** A resource or service provider responsible for delivering any material third party arrangement to the reporting firm/FMI. o **Unknown** o **Other** This is based on the FSB FIRE Taxonomy.
If third party, third party provider name	Required if the incident origin is a third party	If Origin of incident is 'Third Party', the firm must specify the name of the affected third party with which it has an arrangement.
if third party, third party provider LEI	Required if the incident origin is a third party	If Origin of the incident is 'Third Party', the firm may specify the LEI of the service provider. Where an LEI is not available, the firm must enter 'N/A'.
Any supplementary documents	Optional throughout	The firm may include any additional post-incident documentation, as preferred. The field is not mandatory; it will provide the option for firms to include any relevant attachments to the form.

7 Enhanced incident reporting

7.1 This chapter provides guidance for firms in scope of enhanced incident reporting, for an incident that meets one or more of the thresholds in 4.2. We provide guidance on how these firms should submit the 3 phases of an enhanced incident report. We explain how dual regulated firms should consider both FCA and PRA thresholds when assessing an operational incident. We also give examples of operation incidents that meet both regulators' thresholds. Table 2 at the end of this section sets out the enhanced report information field names and explains the information required for each.

Firms in scope of enhanced incident reporting

7.2 The firms in scope of enhanced incident reporting are listed in SUP 15.18.3R, comprising:

- Enhanced scope SMCR firms
- Banks
- Designated investment firms
- Building societies
- Solvency II firms
- CASS large firms
- Payment service providers
- UK RIEs
- Registered trade repositories
- Registered credit rating agencies

How to submit an enhanced incident report

7.3 All firms must submit incident reports via Connect. The system is designed for firms to submit an incident report in phases. The 3 phases are aligned to the Financial Stability Board (FSB) Format for Incident Reporting Exchange (FIRE). Once a firm has created an incident report and submitted the 'initial' phase, it can access the report again to provide a substantial update during the 'intermediate' phase, if necessary. A firm can also provide further updates at this intermediate stage if relevant. Once the firm has resolved the incident, it can close the incident report by adding some extra information, which is the 'final' phase, usually within 30 days. We explain these phases further below. The information required will depend on stage of the report, as set out in Table 2 below.

Initial phase

7.4 Under SUP 15.18.6R and SUP 15.18.7G, a firm must submit the information in the initial phase of an incident report as soon as practicable. We expect the firm this to be within 24 hours of determining that an incident meets any of the thresholds in SUP 15.18.6R(1). This does not mean firms should default to waiting 24 hours to report.

Payment service providers (PSPs)

7.5 In PS26/2 we subsumed the incident reporting requirements under Regulation 99(1) of the Payment Services Regulations into this enhanced reporting framework. PSPs should submit incident reports according to the process outlined in SUP 15.18 and in this document.

7.6 PSPs should follow the same process as other enhanced reporting firms. However, they should submit the initial phase of an incident report within 4 hours of first detecting the incident in line with SUP 15.14.18DD. A report submitted in this way will also serve as a notification under Regulation 99(1) of the Payment Services Regulations. This is the same timeframe required under the EBA's Guidelines on incident reporting under the Payment Services Directive (EBA/GL/2017/10) which previously applied to notifications submitted under Regulation 99(1) of the Payment Services Regulations.

Balancing incident response and reporting

7.7 We know it is difficult for a firm to respond to an incident and report it at the same time. A firm will need to balance the need to report promptly with the need to act to respond to the incident. Firms should consider if an incident is so urgent or significant that it needs to notify its usual supervisory contact as soon as possible, and before submitting a report, for example by phoning or sending an email to its usual FCA supervisory contact. However, it should still submit the reports within the timeframes specified in the rules.

7.8 We will use the information a firm provides at the initial and intermediate phases to help decide if we need to act to manage risks to our statutory objectives. If a firm's answers do not give us enough information, we may need to engage directly. Firms should try to provide what information they can.

Intermediate phase

7.9 Firms should provide one or more updates if there are significant changes to the status of an operational incident. This includes noting that the incident is resolved.

7.10 A firm must provide this information as soon as practicable after there has been a significant change in circumstances from those in the last update it submitted. Some examples of changes that should be reported in this way include:

- The firm identifying the origin of the incident.
- The impact of an operational incident becoming significantly more severe.
- The operational incident meeting another supervisory authority's reporting threshold for submitting an operational incident report after the submission of the initial report to the PRA.
- The firm activating a business continuity plan, disaster recovery plan or making other significant changes to the resolution strategy of the operational incident.
- The firm resolving the operational incident.

7.11 A firm must submit an update each time a significant change occurs. This means that firms may update an incident report more than once as more information becomes available.

7.12 If a firm has resolved an incident before reporting the initial phase information, it may not need to submit the intermediate phase. In this case, a firm can report the incident as resolved in the initial phase and then go straight to the final phase.

Final phase

7.13 A firm must provide a final update within 30 working days of the operational incident being resolved unless there are exceptional circumstances. If a firm cannot do so, it should tell us why and the expected timeline for submission. However, even in cases like this, the firm must submit the final phase as soon as practicable but not more than 60 working days after resolving the incident.

7.14 Scenarios that could mean a firm needs to follow this extended timeframe could include where an incident is so complex that the root cause is not immediately known, or where the firm relies on a third party for the necessary information, and the firm has not been able to receive the information sooner.

Firms regulated by the FCA and the PRA (dual regulated firms)

7.15 Each regulator's thresholds are linked to its statutory objectives. This means a dual regulated firm could experience an incident that equally meets thresholds of both the FCA and the PRA, or one that only meets the thresholds of one regulator. Additionally, an incident could initially meet only one regulator's thresholds for reporting and then evolve to meet the other regulator's thresholds.

7.16 Dual regulated firms will determine whether to notify the FCA, PRA or both, as part of the initial and subsequent stages of its incident report. If a firm submits an incident report only to one regulator, and the incident evolves and meets the other regulator's thresholds, a firm should report this by submitting the 'intermediate' phase. Firms should not create a second initial incident report for the other regulator; only one report is required for both. This is done by selecting the relevant regulators in the incident report.

7.17 Here are some examples of incidents to help dual regulated firms understand how to report:

- **Operational incidents meeting both authorities' thresholds:**

  A cyber incident leads to unauthorised access and theft of data belonging to an end user external to the firm, alongside malicious encryption of critical IT systems. The incident disrupts the delivery of multiple services, leaving end users unable to log into their accounts and complete transactions.

  The firm assesses that it reasonably believes the incident poses a risk of causing intolerable levels of harm to consumers from which they cannot easily recover, meeting the FCA's consumer harm threshold, and poses a risk to the firm's safety and soundness, meeting the PRA threshold.

- **Operational incidents initially meeting a threshold of one authority before the other:**

  A failed IT upgrade causes a technology outage, disrupting access to a firm's insurance claims platform. Major news outlets carry stories on the incident, generating significant negative sentiment on social media.

  The firm reasonably believes the incident risks causing intolerable harm to consumers from which they cannot easily recover, since the incident disrupts

access to a service that helps consumers navigate their financial lives. The firm considers that it meets the FCA consumer harm threshold and reports accordingly.

The incident escalates. The service disruption continues for an extended period, and the firm receives a large number of customer complaints. News outlets report on the incident's escalation.

The firm assesses that, because of the duration of the service disruption, number of customer complaints and severe reputational impact, the incident now could pose a risk to its safety and soundness and financial stability, meeting the PRA reporting thresholds. The firm reports this by providing information in the intermediate phase.

Required information

7.18 The table below is to help firms complete an enhanced incident report in Connect. Please also see this detailed template.

Table 2 – enhanced reporting

Field name	Field Status	Description/Detail required
Authority receiving the report	Required throughout the incident	The firm/FMI must specify the authority to which the report is addressed—such as the Bank of England, the Prudential Regulation Authority (PRA), or the Financial Conduct Authority (FCA). The selected authority must correspond to the trigger identified in the report (e.g., safety and soundness, financial stability, policyholder protection, consumer harm and market integrity, or disruption of an important business service).
Status of the incident	Required throughout the incident	The firm/FMI must select the current status of an incident—open, resolved, or closed. This is based on the FSB FIRE Taxonomy: - **Open:** The period between the time of detection and resolution. The firm/FMI is responding to the incident, minimising impact and prioritising recovery. - **Resolved:** The period between the time of resolution and closure. The immediate impact of the incident has been addressed, though longer-term impacts may take longer to recover from. The firm/FMI is conducting a post-incident review. - **Closed:** The post incident review has been conducted. Findings, remedial activities and lessons learned have been identified.

Trigger for reporting the incident	Required throughout the incident	The firm/FMI must select the criteria that triggered the reporting of the operational incident. The firm/FMI must report to the authorities incidents that the firm/FMI assesses pose a risk to their objectives. This includes: - **Safety and Soundness (PRA/FCA)** - **Financial Stability (PRA/Bank of England)** **- Disrupts Important Business Service (Bank of England)** - **Policyholder Protection (PRA)** - **Consumer Harm (FCA)** - **Market Integrity (FCA)**
Is this a notification under the Payment Services Regulations?	Required throughout the incident	The firm/FMI must select whether the incident report is a notification as a Payment Service Provider to also meet the reporting requirements under regulation 99(1) of the Payment Services Regulations 2017.
Type of incident	Required throughout the incident	The firm/FMI must select the type of incident based on the definition of an operational incident as defined by the authorities. This includes: - **Disruption**: an operational incident that disrupts the delivery of a service to an end user external to the firm; - **Data loss**: an operational incident that impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to such end user.
Incident title	Required throughout the incident	The firm/FMI must add a brief headline to describe unique elements associated with the incident to facilitate reporting and engagement with the authorities. This is intended to be a short reflection of the incident, easy to access and interpret by a broad audience. The headline has the ability to evolve over time to reflect any changes in the firm/FMI's understanding of the incident.
Description of the incident	Required throughout the incident	The firm/FMI must provide any additional details that help describe the incident, including qualitative information on its nature and actions taken or planned for response and recovery, where these are not covered elsewhere in the form. They may also include indicative or confirmed root cause information, with any qualitative description not already captured in other sections.
Firm/FMI severity rating	Required throughout the incident	The firm/FMI must make an assessment of the severity rating of the incident based on its urgency and impact. The firm should make this assessment based on its own internal severity rating and incident

		categorisation, and should use the authorities' reporting criteria based on the FSB FIRE Taxonomy. The severity ratings include: - **Low:** Escalated within relevant functional units. Operational response (eg SOC, operations, technology) is sufficient. - **Medium:** Escalated to invocation of crisis management arrangements. - **High:** Escalated to the most senior level of crisis management command. The firm is activating its most senior command structure.
Time of the detection	Required throughout the incident	The firm/FMI must confirm the time at which the incident has been detected.
Actions planned to recover	Required throughout the incident	The firm/FMI must provide an overview of the planned incident response and recovery strategy, including actions planned to bring the incident under control. In the **intermediate** phase, firms/FMIs must include an update on any significant changes since the previous phase.
Actions taken to recover	Required throughout the incident	The firm/FMI must provide a brief overview of the response or recovery actions already taken to resolve the incident. The firm/FMI must consider adding any relevant information on the technical response or any key decisions taken at a tactical or strategic level. In the **intermediate** and **final** phases, firms/FMIs must include an update on any significant changes since the previous phase.
Estimated time to resolve the incident	Optional throughout the incident	The firm/FMI may provide an estimated timeframe for incident resolution. In the **initial** and **intermediate** phases, the firm/FMI may provide an indicative timeline and indicate the level of confidence in the assessment under the actions taken or planned to recover.
Public reaction to the incident	Optional until the incident is being closed as part of the final report and is then required	The firm/FMI must (may, where optional) provide additional information on any notable negative media or public discourse resulting from the incident. The firm/FMI should use this optional field to provide additional information on customer complaints, press and social media exposure or any relevant public reaction to the incident that might impact the reputation of the firm/FMI. In the **intermediate** and **final** phases, firms/FMIs must include an update on any significant changes since the previous phase.

External communication issued	Optional until the incident is resolved and is then required	The firm/FMI must (may, where optional) describe whether any external communications have been issued. The firm/FMI has the option to share any public statement, official communications or communications to customers impacted in relation to the incident. The firm/FMI should provide any available links as relevant in the field. In the **intermediate** and **final** phases, firms/FMIs must include an update on any significant changes since the previous phase.
Other regulatory bodies notified	Optional until the incident is being closed as part of the final report and is then required	The firm/FMI must (may, where optional) provide a list of all non-financial authorities or relevant agencies (domestic and international) that have been notified of incident. This can include for example (but is not limited to) other non-financial regulatory authorities, such as the Information Commissioner's Office, or relevant law enforcement or governmental agencies such as the National Cyber Security Centre (NCSC) or the National Crime Agency (NCA). In the **intermediate** and **final** phases, firms/FMIs must include an update on any significant changes since the previous phase.
Incident discovery method	Optional in the initial report, but required after or if resolved	The firm/FMI must (may, where optional) indicate the discovery method of the incident. This must be reflective of how the incident was identified or detected by the firm/FMI. This aligns to the FSB FIRE Taxonomy.
Time of the resolution	Required when resolved	The firm/FMI must specify the time at which the impacts associated with incident are brought under control and affected services restored to acceptable levels.
Time of the occurrence (if known)	Optional throughout	The firm/FMI may confirm the time at which the incident is known to have occurred or begun (if known).
Duration of the incident	Pre-populated (Auto-calculated)	The firm/FMI can visualise the overall duration of the incident. This will be calculated automatically and pre-populated for the firm. The form will calculate the difference between 'Time of occurrence', or 'Time of the detection' if occurrence is not available, and 'Time of the resolution'.
Name of the business service affected	Optional in the initial report, but required after or if resolved	The firm/FMI must (may, where optional) include the name of the business service as it is referred to internally. This field is containerised, allowing multiple business services to be listed separately. For each business service listed, the firm can link the following fields individually:

		– Type of the business service affected – Service disruption type – Important business service classification – Proportion of impact tolerance used – Service downtime – Number of users affected – Percentage of users affected – Number of transactions affected – Percentage of transactions affected – Value of transactions affected
Type of the business service affected (Function Category)	Optional in the initial report, but required after or if resolved	For each business service affected, the firm/FMI must (may, where optional) select the type of the business service affected based on the regulated activities impacted by the operational incident or, if applicable, the economic functions to which the service contributes. Note: CF: Central Function, for example HR or payroll BF: Business Function, for example deposit taking.
Service disruption type	Optional in the initial report, but required after or if resolved	The firm/FMI must (may, where optional) select the type of disruption affecting the business services. This includes: - **Availability Loss** (Total, Partial, Intermittent); - **Integrity Loss** (Manipulation, Corruption, Destruction) - **Confidentiality Loss** (Unintended/Unauthorised Disclosure, Unauthorised acquisition). This is based on the FSB FIRE Taxonomy.
Is the affected service classified as an Important Business Service under FCA, PRA or Bank of England rules?	Optional in the initial report, but required after or if resolved	The firm/FMI must (may, where optional) confirm if the affected service is classified as an important business service. Firms in scope of the Operational Resilience rules for the PRA, FCA and Bank of England must select either the 'Yes' or 'No' options to confirm whether the service affected has been classified by the firm/FMI as an important business service. Firms not in scope of the Operational Resilience rules may choose the 'N/A' option.

What proportion of an impact tolerance has been used?	If the service is an Important Business Service, optional until the incident is being closed as part of the final report and is then required	The firm/FMI must (may, where optional) indicate the percentage amount of the impact tolerance used as a result of the incident. This is applicable only if the business service affected is an important business service. The firm/FMI must measure and express in a percentage amount the impact tolerance threshold being measured for the response and recovery operations. This could include the time metric chosen for the important business service, but it could also include other relevant metrics used by the firm/FMI to determine the impact tolerances. Some high level examples include (but are not limited to): - The time metric of the impact tolerance is 24 hours. If the operational incident has lasted for approximately 4 hours, the firm/FMI would have used 16% of the impact tolerance. - The customer complaints metric of the impact tolerance is set at 500 customer complaints. Having received 150 complaints, the firm/FMI has used 30% of its impact tolerance. - The availability metric of the impact tolerance is set at 100 failed transactions. With 25 missed transactions, the firm/FMI has used 25% of its impact tolerance. In the **final** phase, the firm/FMI must include the total impact tolerance used until service was restored or the immediate impact of the operational incident was mitigated.
Service downtime	Required when resolved	The firm/FMI must specify the (minimum) time period from service being fully or partially unavailable to external end-users until regular activities or operations have been restored.
Number of affected customers	Not visible for initial report. Optional after the initial report until the incident is being closed as part of the final report and is then required; unless the incident is being reported under PSR when it is required after the initial report (including if resolved).	The firm/FMI must (may, where optional) include the (approximate) total number of end users external to the firm affected for a specific service. At both the **initial** (resolved) and **intermediate** phases, this field is mandatory for firms reporting under their PSD2 requirements.
Percentage of service users affected	Not visible for initial report. Optional after the initial report until the incident is being closed as part of the final report and is then required; unless the incident is being	The firm/FMI must (may, where optional) include the percentage of specific service's user base affected relative to total. The firm/FMI can express the figure in a percentage format.

	reported under PSR when it is required after the initial report (including if resolved).	At both the initial (resolved) and intermediate phases, this field is mandatory for firms reporting under their PSD2 requirements.
Percentage of transactions affected	Not visible for initial report. Optional after the initial report until the incident is being closed as part of the final report and is then required; unless the incident is being reported under PSR when it is required after the initial report (including if resolved).	The firm/FMI must (may, where optional) include the percentage of transactions affected relative to total. The firm/FMI can express the figure in a percentage format. At both the **initial** (resolved) and **intermediate** phases, this field is mandatory for firms reporting under their PSD2 requirements.
Value of transactions affected	Not visible for initial report. Optional after the initial report until the incident is being closed as part of the final report and is then required; unless the incident is being reported under PSR when it is required after the initial report (including if resolved).	The firm/FMI must (may, where optional) include the value of transactions affected for a specific service. If the operational incident is not resulting in disruption to transactions, the firm/FMI may add '0' as a value. At both the **initial** (resolved) and **intermediate** phases, this field is mandatory for firms reporting under their PSD2 requirements.
Number of transactions affected	Not visible for initial report. Optional after the initial report until the incident is being closed as part of the final report and is then required; unless the incident is being reported under PSR when it is required after the initial report (including if resolved).	The firm/FMI must (may, where optional) include the number of transactions affected for a specific service. If the operational incident is not resulting in disruption to transactions, the firm/FMI may add '0' as a value. At both the **initial** (resolved) and **intermediate** phases, this field is mandatory for firms reporting under their PSD2 requirements.
Level of geographic spread	Optional in the initial report, but required after or if resolved	The firm/FMI must (may, where optional) provide an indication of how widespread the geographical impact of the incident might be. This can include: - **Local:** the impact is within the same urban centre - **Regional:** the impact is limited to territorial divisions within a jurisdiction (e.g. counties, municipalities) - **National:** the impact has been identified through a single jurisdiction. - **Multi-jurisdictional:** the impact has been assessed through multiple jurisdictions - **Global:** the impact has been identified across a majority of jurisdictions in multiple continents.

		This is based on the FSB FIRE Taxonomy. The geographical spread might change as response and recovery operations progress.
Affected party type(s)	Optional until the incident is being closed as part of the final report and is then required	The firm/FMI must (may, where optional) specify the types of parties directly affected by the service disruption from the reporting firm/FMI. This includes: - **Entities within the group:** Another firm/FMI within the same group affected by the incident (other than the reporting firm/FMI). - **Business counterparties:** a separate financial institution with which the reporting firm/FMI has a pre-existing relationship - **Third party vendor or service providers:** a service provider responsible for delivering any third party arrangement to the reporting firm/FMI. - **Customer/consumers:** Affected customers/consumers, as defined in the PRA Rulebook and FCA Handbook, and for Bank firms, participants or clearing members as relevant. - **Vulnerable customers:** affected vulnerable customers as defined in the FCA Guidance (FG21/1). - **General Public:** people/individuals in society with no relationship to the reporting entity or entities within the same group. - **Other financial market participants:** separate financial entities affected by the incident (not captured by the other categories) - **Other:** other non-financial entities not included by other categories. - **None:** No other entities affected by the incident. This is based on the FSB FIRE Taxonomy.
Related affected entities	Optional until the incident is being closed as part of the final report and is then required	The firm/FMI must (may, where optional) provide a list of all entities related to the reporting firm/FMI affected by the incident within the same organisation. The firm/FMI has an option to include a LEI identifier to facilitate identification of firm/FMI. Where an LEI is not available, the firm/FMI can supply a Companies House number as an alternative. Where the Service Provider has no identifier, the firm/FMI can use a free option to provide relevant information or enter 'N/A'.
Cause type	Optional until the incident is being closed as part of the final report and is then required	The firm/FMI must (may, where optional) select the root cause of the incident. During the **initial** and **intermediate** phases, the firm/FMI may provide an indicative root cause of the operational incident. In the **final**

		phase, the firm/FMI must include the confirmed root cause of the operational incident, as outlined in the post-incident review.
Origin of the incident	Optional in the initial report, but required after or if resolved	The firm/FMI must (may, where optional) select a high level categorisation of the incident origin. This should include whose or what actions cause or contributed to the operational incident. o **Internal**: A firm/FMI resource employed directly by the firm/FMI o **External**: A resource with no relationships with the firm/FMI o **Third Party**: A resource or service provider responsible for delivering any material third party arrangement to the reporting firm/FMI. o **Unknown** o **Other** This is based on the FSB FIRE Taxonomy.
If third party, third party provider name	Required if the incident origin is a third party	If Origin of the incident is 'Third Party', the firm/FMI must (may, where optional) specify the name of the affected third party with which it has an arrangement.
Third party provider Legal Entity Identifier	Required if the incident origin is a third party	If Origin of the incident is 'Third Party', the firm/FMI must specify the LEI of the service provider. Where an LEI is not available, the firm/FMI must enter 'N/A'.
Time of the closure	Not visible until the incident is being closed as part of the final report when it is required	The firm/FMI must confirm the date and time when the incident was closed.
Type of resource affected	Not visible until the incident is being closed as part of the final report when it is required	The firm/FMI must describe the properties of the resources affected by the operational incident. The firm/FMI must choose from a list of resource types. This aligns with the FSB FIRE Taxonomy.
Resource affected properties	Not visible until the incident is being closed as part of the final report when it is required	The firm/FMI must describe the properties of the resources affected by the operational incident. This aligns with the FSB FIRE Taxonomy.

Describe the lesson identified	Not visible until the incident is being is being closed as part of the final report when it is required	The firm/FMI must describe the key findings contained in the post-incident review. This should include a summary of lessons identified during the post-incident review.
Describe the remedial action being taken	Not visible until the incident is being closed as part of the final report when it is required	For each lesson identified, the firm/FMI must include an overview of the remediation actions identified as part of the post-incident review. The firm/FMI must include the estimated date for completion of the remediation activity for each action identified.
Any supplementary documents	Optional throughout	The firm/FMI may include any additional post-incident documentation, as preferred. The field is not mandatory; it will provide the option for firms/FMIs to include any relevant attachments to the form.