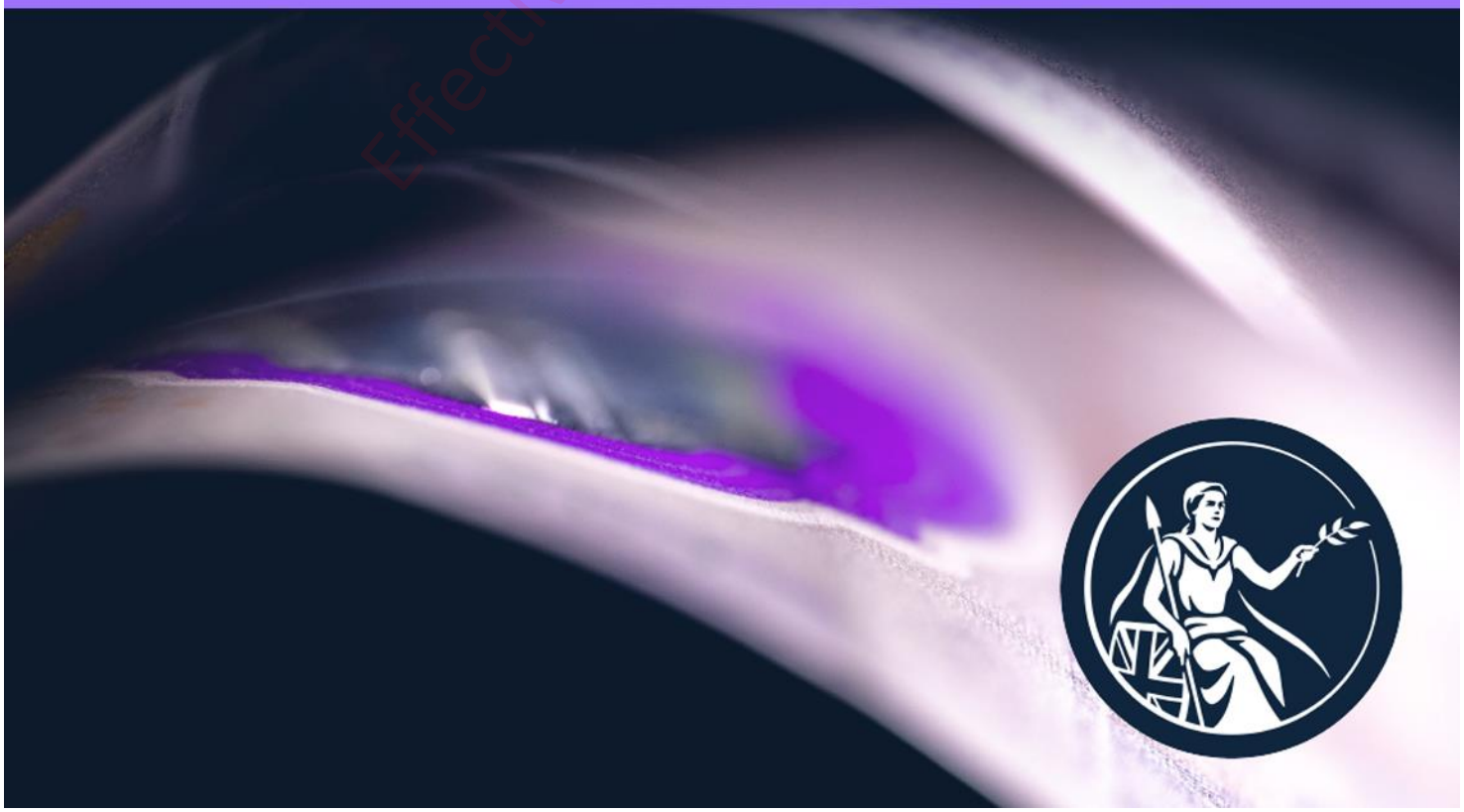
Bank of England PRA

# SS1/26 – Operational resilience: Incident reporting



**Supervisory statement | SS1/26**

March 2026



**Bank of England | Prudential Regulation Authority**

# Operational resilience: Incident reporting

## Supervisory statement | SS1/26

**March 2026**





Prudential Regulation Authority | 20 Moorgate | London EC2R 6DA

# Contents

# 1: Introduction

1.1 This supervisory statement (SS) sets out the PRA's expectations of how firms should comply with the requirements in the PRA Rulebook for reporting an operational incident.

1.2 These requirements seek to support the operational resilience of the UK financial sector by collecting information from firms on operational incidents which pose a risk to the safety and soundness of firms, policy holder protection or UK financial stability. Further, the aim of the incident reporting policy is to set out clear and consistent reporting requirements and expectations for firms for when they experience an operational incident.

1.3 This SS is relevant to all:

- UK banks, building societies, PRA-designated investment firms, UK branches of overseas banks (hereafter banks); and
- UK Solvency II firms, the Society of Lloyd's, and its managing agents (hereafter insurers).

1.4 Banks and insurers are collectively referred to as 'firms' in this SS.

1.5 The expectations set out in this SS should be read in conjunction with:

- the Regulatory Reporting Part of the Rulebook;
- the Operational Resilience Part of the PRA Rulebook, Insurance-Operational Resilience Part of the PRA Rulebook and SS1/21 –Operational resilience: Impact tolerances for important business services;
- the Fundamental Rules Part of the PRA Rulebook; and
- the Notifications Part of the PRA Rulebook.



## Structure of this SS

- Chapter 2 – sets out how a firm should comply with the incident definition requirements.
- Chapter 3 – sets out how a firm should comply with the incident reporting threshold requirements.
- Chapter 4 – sets out how a firm should comply with the phased approach to incident reporting.
- Chapter 5 – sets out how a firm should comply with the governance expectations.

# 2: Operational incident definition

2.1 This chapter sets out the PRA expectations on what constitutes an operational incident as set out in Chapter 1.2 of the Regulatory Reporting Part of the PRA Rulebook.

2.2 The PRA has defined an operational incident as 'either a single event or a series of linked events which disrupts the firm's operations such that it:

(1) disrupts the delivery of a service to an end user external to the firm; or
(2) impacts the availability, authenticity, integrity or confidentiality of information or data relating or belonging to such end user'.

2.3 The PRA considers a 'series of linked events' to include those whose cumulative impact result in a disruption to the firm's operations. This could include an event having cascading effects or multiple events originating by the same root cause. Examples can include but are not limited to:

- 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 delays 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.

2.4 Firms should consider whether the end user external to the firm is identifiable, in line with SS1/21 – **Operational resilience: Impact tolerances for important business services**. This may include retail customers, business customers, other legal entities, trustees, market participants, the supervisory authorities or other members of a regulated entity's group.

2.6 The PRA requires firms to assess whether an incident meets the definition of an operational incident regardless of whether this impacted the delivery of an important business service, or data associated with an important business service.

2.7 The PRA considers that an operational incident that does not impact the delivery of an important business service can pose a risk to its objectives. Examples of such incidents may include but are not limited to:

- 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 confidence among financial counterparties or customers to deteriorate, leading them to exit relationships with the firm and risking its safety and soundness.
- An IT failure affecting the 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.

2.8 The PRA requires firms to submit a report if an incident meets either one or both criteria in the definition of an operational incident and meets the PRA thresholds. A potential or uncrystallised event, which does not result in a disruption to a service or result in data loss to an end user external to the firm, would be considered a near-miss and fall outside the scope of reporting.

# 3: Operational incident reporting thresholds

3.1 This chapter sets out the PRA's expectations for how firms should interpret the thresholds set out in 24.2 of the Regulatory Reporting part of the PRA Rulebook.

3.2 Firms must submit an operational incident report if an operational incident could pose a risk to:

(1) where the firm is, or is controlled by, an O-SII or is a relevant Solvency II firm,[1] the stability of the UK financial system;

(2) the firm's safety and soundness; or

(3) an appropriate degree of protection for those who are or may become the firm's policyholders (insurers only).

3.3 When assessing whether an operational incident meets [one or more of] the threshold[s] and must be reported to the PRA, firms could consider a range of factors. This may include, but is not limited to:

- operational and financial contagion (O-SIIs/relevant Solvency II firms only);
- the firm's or, if an O-SII/relevant Solvency II firm, the sector's reputation;
- 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 data or information relating or belonging to an end user external to the firm; and
- the firm's internal assessment and classification of the incident.

3.4 The PRA anticipates that most firms will build consideration of the PRA's thresholds into existing internal incident reporting processes. The factors, covered in more detail in the following subsections, provide guidance on how firms may interpret the thresholds. They are not exhaustive or prescriptive. These factors serve as examples of how a firm should consider the PRA's reporting thresholds. Firms may alternatively use existing metrics employed within their internal processes.

3.5 Firms may use existing internal processes to determine the scale and potential impact of an incident to help assess whether it meets the PRA's thresholds for reporting. The PRA recognises that, in the early stages of incident response, a firm may not have a complete view of the incident's long-term implications. The threshold assessment can only be based on the information available at the time and judgement will be required.



[1] As defined in the Glossary of the PRA Rulebook.

3.6 Examples of operational incidents that firms may report to the PRA include, but are not limited to:

- **Cyber attacks, such as:**
  - A phishing attack on a firm which compromises the confidentiality of sensitive or critical data belonging to an end user external to the firm.
  - A large-scale distributed denial of service (DDoS) attack on a cloud service provider which causes significant disruption to the delivery of one or more of a firm's services.
- **Process failures** which significantly disrupt the delivery of a service, for example, in the case of a deposit taker, the prevention or delay of a significant number of payments.
- **System update failures** which result in significant disruption of one or more services, for example, in the case of an insurer, the firm being unable to pay out a significant number of annuity payments.
- **Infrastructure problems**, including extended power outages or infrastructure damage from extreme weather, which results in a firm being unable to provide one or more of its services. For example, a physical break in a fibre connection at a site resulting in a firm's online services being unavailable for an extended period.

3.7 A firm may assess that an operational incident meets the thresholds for reporting to both the PRA and FCA, depending on the specific circumstances of an incident. If a firm submits information to one supervisory authority, and the incident evolves and meets the other authority's thresholds, a firm should report this by submitting information at the intermediate phase. Examples may include but are not limited to:

- **Operational incidents meeting both authorities' thresholds:**
  A cyber incident leads to unauthorised access and exfiltration 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 'consumer harm' threshold, and could pose a risk to the firm's safety and soundness, meeting the PRA reporting threshold.

- **Operational incidents initially meeting one authority's thresholds before the other's**:
  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 poses a risk of 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.

The following sub-sections provide additional guidance on the threshold factors.

## Operational and financial contagion

3.8 O-SII and relevant Solvency II firms are required to submit an operational incident report when an operational incident poses a risk to financial stability. As set out in **the FPC's macroprudential approach to operational resilience**, when determining the potential impact on financial stability, firms should consider whether there is a risk of operational contagion or financial contagion.

3.9 As set out in paragraph 2.5 of SS1/21, the PRA expects O-SII and relevant Solvency II firms to assess the risk a business service poses to financial stability, specifically where there is the potential to cause knock-on effects for counterparties, particularly those that provide financial market infrastructure or critical national infrastructure. Firms may leverage these assessments to determine whether an operational disruption could have a contagion effect on their clients, other market participants, FMIs and the wider UK economy. The PRA does not expect firms in the early stages of an incident to assess the total impact an operational incident may have on the wider system.

3.10 Examples include, but are not limited to, a software failure resulting in disruption to a payment processing service and causing knock-on effects on payments across multiple firms, resulting in significant liquidity shortages; a cyber incident affecting a firm's outsourced claims processing services resulting in disruption in the delivery of services across multiple insurers and impacting their ability to manage their own risks.

## The firm or the sector's reputation

3.11 Firms are expected to submit an operational incident report where an operational incident risks its own reputation or, if an O-SII/ relevant Solvency II firm, the reputation of the financial sector, therefore risking the safety and soundness of the firm, policyholder protection or financial stability.

3.12 Firms should consider whether an operational incident could result in a loss of confidence in the firm itself or, if an O-SII/ relevant Solvency II firm, the wider financial sector. This could include, where an operational incident causes a firm's counterparties or customers to revise their view of the firm, the riskiness of the firm, its ability to manage its risks and the risks to its business model, or the strength of the financial markets.

3.13 Examples may include, but are not limited to, a technology outage preventing users from accessing their bank accounts or claims portals, resulting in negative sentiment in news outlets and social media and prompting users to leave the firm; or a third-party process failure, resulting in the corruption of critical data belonging to an end user external to the firm, prompting financial counterparts to stop transacting with the firm.

## The firm's ability to meet its legal and regulatory obligations

3.14 The PRA expects a firm to submit an operational incident report where an operational incident could result in the firm failing to meet its legal and regulatory obligations.

3.15 Firms are expected to consider whether the incident would lead to heightened regulatory monitoring, formal regulatory action, or authority intervention. This could include, but is not limited to, where the delivery of an important business service is disrupted, or the risk of a firm being unable to remain within impact tolerances, or when the firm fails to comply with the PRA's threshold conditions or fundamental rules.

3.16 Examples include but are not limited to a third-party failure resulting in loss of critical data, leaving a firm unable to fulfil contractual obligations such as processing insurance claims, settling payments, or providing timely disclosures to clients.

## The firm's ability to provide adequate services

3.17 The PRA expects a firm to submit an incident report where an operational incident could result in significant disruption to the service. A firm is expected to consider whether disruption arising from operational an incident is such that its ability to deliver services adequately may be called into question, leading to potential loss of business and damaging revenues.

3.18 This could include, but is not limited to:

- the firm being unable to provide a business service (or services) for an extended period of time, particularly in the case where important business services are disrupted;
- the firm being unable to meet contractual obligations;
- the firm being unable to complete or process a significant number of transactions; and
- a disruption causing mounting detriment or actual harm to customers or clients.

## The firm's ability to safeguard the availability, authenticity, integrity or confidentiality of data or information relating or belonging to an end user external to the firm.

3.19 The PRA expects a firm to submit an operational incident report where an operational incident could compromise the firm's ability to safeguard information and data belonging to an end user external to the firm, this would include data or information:

- becoming temporarily or permanently inaccessible or unusable;
- having questionable authenticity, for example, a data source becoming untrustworthy;
- becoming inaccurate or incomplete; or
- being accessed by or disclosed to an unauthorised party or system.

3.20 Examples include, but are not limited to, unauthorised access to data or a loss in sensitive data belonging to an end user external to the firm, a cyber-attack on the firm, or an internal service error resulting in a loss of data belonging or relating to an end user external to the firm.

## The firm's internal assessment and classification of the incident

3.21 A firm must submit an operational incident report where the operational incident meets the threshold set by the PRA. Where a firm has assessed an operational incident as high priority according to its own internal procedures, this may be indicative that the PRA's threshold has been met. Additionally, where an operational incident has resulted in the formal activation of a high level of internal escalation, such as escalation to senior management, the Senior Manager Function (SMF)24, or the Board, this is likely to be indicative that the PRA's threshold has been met.

3.22 Examples include but are not limited to: a firm activating its crisis management arrangements and standing up its tactical or strategic response; or a firm categorising an operational incident as a 'Priority' critical incident, according to its own internal classification methodology.

# 4: Approach to phased incident reporting

4.1 When an operational incident meets a threshold, under Chapter 24 of the PRA's Regulatory Reporting Part a firm is required to:

- Submit to the PRA the information specified at the initial phase in the Reporting Fields Document, as soon as is practicable after the occurrence;
- Submit the information specified at the intermediate phase in the Reporting Fields Document as soon as is practicable after any significant change in circumstances from that described in the initial phase; and
- Submit the information specified at the final phase in the Reporting Fields Document within 30 working days or, where this is impracticable, as soon as is practicable but not exceeding 60 working days of the operational incident being resolved.

4.2 Chapter 24 of the PRA's Regulatory Reporting Part requires a firm to complete all the required information at each reporting phase. While not required, the PRA expects firms to provide optional information in the report, where this is available. In the event that an incident originates at a third party, the PRA expects a firm to take reasonable steps to obtain information regarding the root cause of the incident from the third party.

4.3 Firms are expected to use FCA Connect to complete the report submission.

4.4 Notwithstanding the above, a firm continues to be required to notify the PRA of incidents that may constitute 'information of which the PRA would reasonably expect notice' within the meaning of Fundamental Rule 7. The requirement set out Chapter 24 of the PRA Regulatory Reporting Part to submit an incident report does not replace the General Notification Requirements in Chapter 2 of the Notification Part. Operational incident reporting should not replace all supervisory engagement during an incident and direct communication with supervision teams may still be needed depending on the incident.



## Initial phase

4.5 Chapter 24 of the Regulatory Reporting Part of the PRA Rulebook requires firms to submit the information specified in the Reporting Fields Document as soon as practicable after an operational incident has occurred and met one or more of the thresholds in Regulatory Reporting Rule 24.2 and described in Section 2. The PRA would expect a firm to submit a report within 24 hours of determining an incident has met a threshold. The PRA acknowledges that where an incident requires all the firm's resources to address the incident, the firm may take longer than 24 hours to submit a report.

4.6 A firm should balance the need to submit an incident report to the PRA with prioritising the necessary actions to resolve and recover from the operational incident.

4.7 A firm should take reasonable steps to collect the best available data at the time of submission. The PRA acknowledges that a firm may gain a more accurate view of the impact of disruption as the resolution of the incident progresses.

## Intermediate phase

4.8 Rule 24.3 requires a firm to submit the additional information specified in the Reporting Fields Document as soon as practicable after there has been a significant change in circumstances from that described in the last submission. Under Chapter 24 of the Regulatory Reporting Part of the PRA Rulebook, firms are required to submit information to keep the PRA informed of any significant changes in circumstances regarding the operational incident in as soon as practicable and provide further details on the incident as well as any actions the firm is taking to resolve/remediate the impact of it.

4.9 A significant change in the incident could include a change in impact or the status of the incident. Examples of where firms should update the report at the intermediate phase include, but are not limited to:

- The firm identifying the origin of the incident.
- The impact of an operational incident becoming significantly more severe.
- The operational incident meeting another supervisory authorities' 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.

4.10 Under Rule 24.3, a firm is required to submit the information specified for the intermediate phase each time a significant change occurs; therefore, firms may be required to provide further information more than once. A firm is required to submit information at the intermediate phase at least once to inform the PRA that it has resolved the operational incident.

4.11 In the event that a firm has resolved an incident prior to submitting a report in the initial phase, an update in the intermediate phase may not be necessary. A firm can indicate it has resolved the incident in the initial phase and proceed to completing the report in the final phase.

4.12 A firm should update the report only including new information or data not previously submitted to the PRA in the intermediate phase, prioritising significant changes to the circumstances of an operational incident.

4.13 A firm should balance the need to submit an incident report to the PRA with prioritising the necessary actions to resolve and recover from the operational incident.

## Final phase

4.14 Once an operational incident has been resolved, under Rule 24.4 a firm is required to submit the information specified at the final phase in the Reporting Fields Document within 30 working days, where this is impracticable, as soon as is practicable but not exceeding 60 working days.

4.15 The PRA expects a firm to submit the final update within 30 working days unless there are circumstances which would necessitate further time to collect all the information required in the final report. Reasons for such a delay could include where an incident is so complex that the firm does not immediately know the root cause, or where the firm relies on a third party for the necessary information.

4.16 Firms are expected to inform the PRA when it is impracticable to submit the final update within 30 working days, explaining the reason as to why it is impracticable and the expected timeframe for the submission of the final report update.

# 5: Governance

5.1 The PRA expects firms to establish clear accountability and responsibility for meeting the outcomes of the policy. Firms should align the allocation of senior management responsibilities for operational incident reporting with the expectations set out in Chapter 7 of SS1/21 and, for incidents involving third-party service providers, Chapter 4 of SS2/21.

5.2 The PRA expects the Chief Operations Senior Management Function (SMF)24, where it exists, to hold overall responsibility for implementing the outcomes of the PRA's incident reporting requirements and expectations, and for ensuring that the firm's internal processes enable the accurate and timely reporting of operational incidents that meet the thresholds in the PRA's rules. Where a firm does not have an SMF24, a firm should clearly allocate these responsibilities to a suitable SMF or SMFs.

5.3 While the PRA expects clear accountability for these outcomes, it does not expect the SMF24 or, if different, the responsible SMF to approve the submission of incident reports. The PRA expects firms to structure oversight of operational incident reporting in the most effective way for their business, considering existing governance structure.