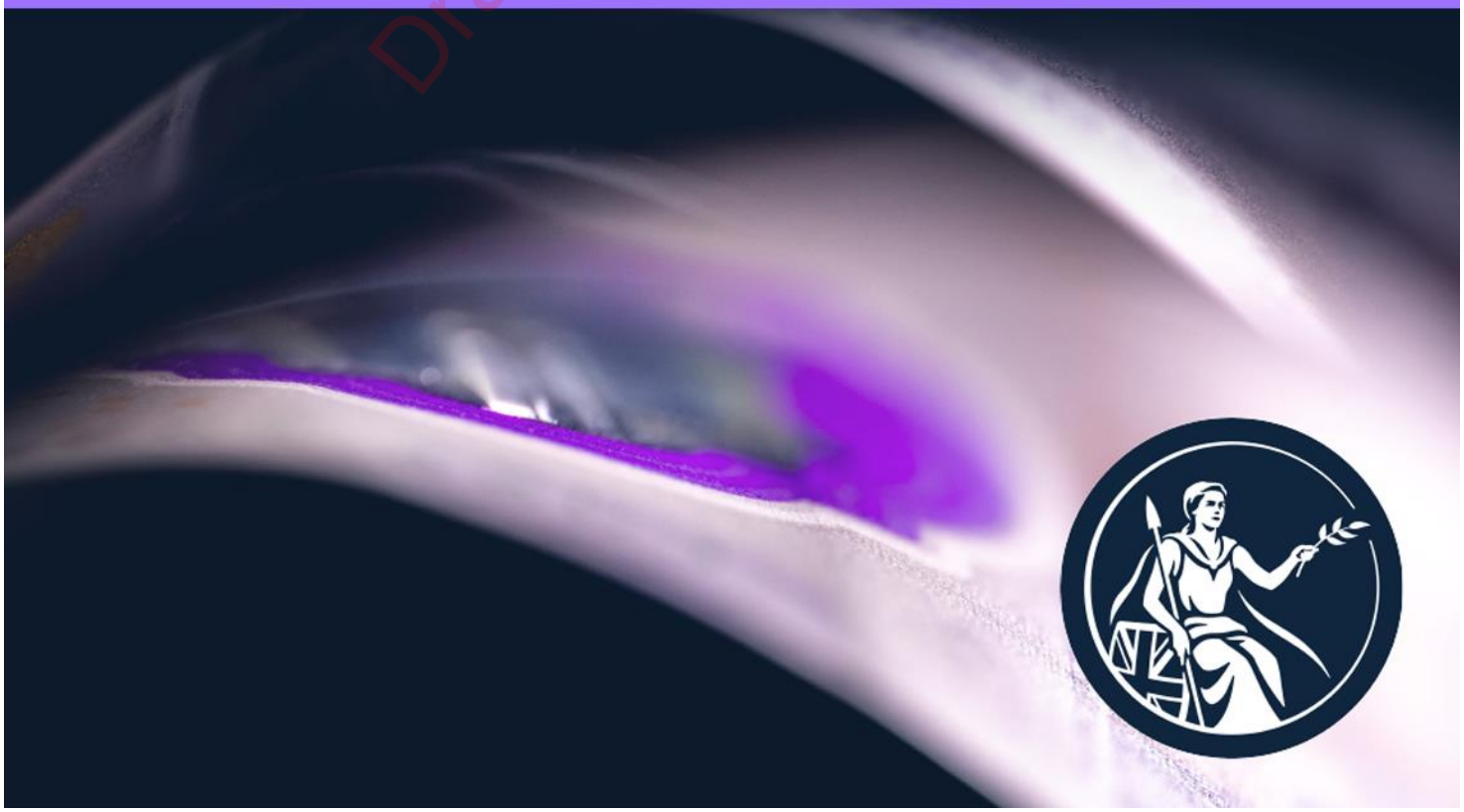
Bank of England PRA

Operational Resilience: Incident Reporting

Draft supervisory statement

December 2024



Bank of England | Prudential Regulation Authority

Operational Resilience: Operational Incident Reporting

Supervisory statement | SSXX/XX

December 2024

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 supervisory statement

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

2. Operational Incident reporting thresholds

2.1 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.

2.2 Firms must submit an operational incident report in the event that 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).

2.3 When assessing whether an operational incident meets the threshold and must be reported to the PRA, the PRA would expect firms to consider a range of factors. This could 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.

These elements are covered in more detail in the following sub-sections.

2.4 Examples of operational incidents which the PRA would expect firms to report 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.

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

- **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.

Operational and financial contagion

2.5 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 are expected to consider whether there is a risk of operational contagion or financial contagion.

2.6 The PRA expects O-SII and relevant Solvency II firms to consider operational contagion, where an operational incident could cause operational disruption elsewhere in the financial system or the real economy. An operational incident affecting the services of an O-SII firm or relevant Solvency II firm could leave them unable to transact with other firms or participate in financial markets. This could have knock-on impacts on the ability of the disrupted firm's counterparties to undertake their own activities.

2.7 O-SII/relevant Solvency II firms should consider whether an operational incident could result in further financial impacts on the firm or the financial sector. This includes, but is not limited to, an impact on liquidity flows, access to funding sources, price discovery in certain markets or for particular assets, or a firm's ability to make margin payments to a certain central counterparty (CCP), triggering default proceedings.

The firm or the sector's reputation

2.8 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.

2.9 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 market.

2.10 As part of its assessment of whether an incident should be reported to the PRA, firms should consider whether the incident has, or is likely to:

- have significant coverage in the media, including, but not limited to, social media, local and national news;
- lead to the firm receiving repetitive complaints from customers or financial counterparts; or
- risk the firm losing customers or financial counterparts with a material impact on its business because of the incident.

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

2.11 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.

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

The firm's ability to provide adequate services

2.13 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.

2.14 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 assets relating or belonging to an end user external to the firm.

2.15 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.

2.16 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

2.17 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 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. Approach to phased incident reporting

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

- An initial incident report;
- One or more intermediate reports if there has been a significant change; and
- A final report.

3.2 Chapter 24 of the PRA's Regulatory Reporting Part requires a firm to complete all the required information in the incident reports. Firms are able to provide optional further information in the report where relevant. 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.

3.3 Firms are expected to use the FCA's Connect Portal to complete the report submission.

3.4 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.

Initial operational incident report

3.5 Chapter 24 of the Regulatory Reporting Part of the PRA Rulebook requires firms to submit an incident report 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 breached 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.

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

Intermediate operational incident report

3.8 Rule 24.3 requires a firm to submit an intermediate report as soon as practicable after there has been a significant change in circumstances from that described in the last incident report submitted by the firm. Under Chapter 24 of the Regulatory Reporting Part of the PRA Rulebook, firms are required to submit one or more intermediate reports to keep the regulators 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.

3.9 A significant change in the incident could include a change in impact or the status of the incident. Examples of where firms should submit an intermediate report include, but are not limited to:

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

3.10 Under Rule 24.3, a firm is required to submit an intermediate report each time a significant change occurs, therefore, firms may be required to submit multiple intermediate

reports. At least one intermediate report is required to inform the PRA once the firm has resolved the operational incident.

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

3.12 In the event that a firm has resolved an incident prior to submitting an initial report, they are not required to complete an intermediate report and can move straight to the final report stage.

Final operational incident report

3.14 Once an operational incident has been resolved, under Rule 24.4 a firm is required to submit a final report to the PRA within 30 working days, where this is impracticable, as soon as is practicable but not exceeding 60 working days.

3.15 The PRA expects a firm to submit an incident report within 30 working days unless there are circumstances which would necessitate further time to collect all the information required in the final report. This could include, but is not limited to, where an incident is of such complexity that further time is required to substantiate the root cause of an incident, or where a firm is reliant on another party to complete the necessary information, such as a third party.

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