FSB FINANCIAL STABILITY BOARD

15 April 2025

Format for Incident Reporting Exchange (FIRE)

Overview of responses to the consultation

Introduction

The public consultation for FIRE was open between 17 October and 19 December 2024 and yielded responses from 16 stakeholders across the banking, insurance, asset management and financial market infrastructures sectors. Respondents ranged from individual financial institutions to associations and think tanks.

Overall, there was strong support for the objectives of FIRE, particularly its goals of promoting convergence and flexibility in incident reporting frameworks. Respondents emphasised the importance of public-private partnership in enhancing cyber and operational resilience and appreciated the inclusive process. One respondent noted the need for continued engagement between FSB members and non-FSB member jurisdictions, other global standard-setters, and industry to help support adoption. Respondents appreciated the flexibility and customisation options offered by FIRE, allowing varying levels of adoption and promoting convergence across frameworks. They also valued FIRE's comprehensive coverage of operational and cyber incidents, as well as its potential applicability to third-party service providers and other sectors.

At the same time respondents highlighted the challenges associated with broad and immediate adoption, suggesting phased implementation and alignment with existing frameworks like the European Union's Digital Operational Resilience Act (DORA). Concerns were raised regarding the confidentiality of incident reports and potential legal liabilities, highlighting the need for clear guidelines and protections. Additionally, there was consideration of implementation costs and operational challenges, with recommendations for cost-benefit analysis.

The overview of responses is set out in three sections: i) general comments on FIRE, which resulted in the inclusion of clarifying language; ii) changes made to the information items, which resulted in a net reduction in the number of information items; and iii) other feedback received which highlighted the need for further clarifications.

1. General comments on FIRE

1.1. Confidentiality of incident reports

Several respondents raised the importance of ensuring confidentiality of incident reports. Some respondents raised concerns about the confidentiality of shared information, potential legal liabilities from incorrect disclosures, and the burden of reporting less relevant incidents. One respondent noted some national legal frameworks provide additional protections for reporting

entities, such as barring reported information from being used in regulatory enforcement actions, preserving attorney-client privilege, and prohibiting the use of reported information in legal proceedings. Another respondent raised the issue of conflicting compliance requirements across jurisdictions. Concerns about incident forwarding and the sensitivity of data shared with regulators were also noted.

Authorities already ensure the confidentiality of sensitive information with various measures and controls. Although specific security measures are outside the scope of FIRE, the importance of confidentiality is emphasised given the sensitivity of data reported using FIRE. To address these concerns, additional language was included to clarify that authorities should share information with other authorities based on existing information sharing arrangements for confidential and sensitive information. In response to another comment, the final FIRE version clarifies that the FSB does not collect incident reports.

1.2. Reporting phase clarification

The FSB clarifies that while the FIRE format supports the common three-phase reporting (initial, intermediate, final), it can also accommodate two-phase and single-phase reporting if preferred locally.

2. Changes to information items

2.1. Information items added

During the public consultation, the FSB also tested the robustness of the FIRE framework using sanitised data from industry stakeholders. The testing aimed to ensure that FIRE is practical and effective in real-world scenarios.

Most issues identified during testing were resolved through changes proposed by respondents. However, some issues arose during the validation process that required further adjustments. Namely, certain information items were too complex to validate in their original form.

To simplify complex information items, the FSB broke these down into additional more manageable items, resulting in three new items:

- **FIRE report language.** Originally a single item, it was split into three separate items for better clarity and validation: FIRE report language **code**, FIRE report language **country** and FIRE report language **customisation**.
- **impact geographic spread**. An additional item was created to describe the specific jurisdictions where the effects of the incident are being experienced. This provides more detailed information about the geographic impact of the incident**.**

2.2. Information items removed

In reviewing the balance between FIRE's flexibility and convergence objectives, a total of 15 information items have been removed.

To reduce the reporting burden for entities, the FSB has removed the fields providing the “max” values. It is understood that these information items are likely to contain best guesses or estimates during the reporting lifecycle and may only be fully known after the incident has been resolved. In addition, all the ‘peak’ information items were removed in response to feedback indicating that the concept of "peak" impact is subjective and challenging to assess, as it is difficult to determine the exact timing of the peak. The FSB acknowledges that this information can be derived from the impact scale fields reported in the previous phases. The removed ‘max’ and ‘peak’ fields are as follows:

- incident estimated resolution timeframe max
- service downtime max
- affected end user number max
- affected end user percentage max
- affected transaction number max
- affected transaction percentage max
- affected transaction value max
- impact financial loss max
- impact financial peak
- impact operational peak
- impact reputational peak
- impact legal / regulatory peak
- impact external peak

Some respondents found the impact scales complicated and difficult to assess while reporting, adding confusion rather than value. Specifically, the Legal/Regulatory impact scale required speculation on potential breaches of contracts or regulatory non-compliance. The FSB acknowledges these concerns and has removed the **Legal/regulatory impact scale**. Financial entities can now provide relevant contextual information, if available, under the field “impact notes” without adhering to predefined criteria or engage in speculation.

A few respondents raised concerns about the sensitivity of information and potential legal exposure related to the ‘vulnerabilities exploited’ item. They noted that a similar field was removed during the DORA consultation process. To reduce the reporting burden and align with existing practices in different jurisdictions, ‘**vulnerabilities exploited**’ has been removed from the FIRE design.

2.3. Information items clarified

A number of comments were received that asked for greater clarification on several information items.

- **recipient identifier(s).** There was broad agreement among respondents that the FIRE design facilitates incident reporting by third-party service providers to financial institutions and valued the guidance on differentiating between individual and broad-based communications using the 'recipient identifier(s)' information item. Supplemental guidance for how to differentiate between individual and broad-based communications has been included, whereby the 'recipient identifier(s)' information item can also be used to describe a specific cohort of receiving entities rather than only individual entities.

- **public reaction.** Additional guidance has been included confirming that the intent is to receive information uniquely provided by the reporting entity, such as their perspective on external stakeholder perceptions or interactions with end users (e.g. call centre).

- **communications issued.** Respondents compared the 'comms issued' item in FIRE to the removal of a similar field in the DORA Incident Reporting RTS. Although similar, the FIRE field covers a broader scope of communications, covering communications involving a greater diversity of jurisdictions. Further guidance clarifies that this item focuses on broad-based statements issued publicly or privately, rather than bespoke bilateral interactions with individual affected parties. This guidance aims to reduce the sensitivity related to notifications to specific external end users.

- **affected parties.** Some respondents recommended streamlining the "Affected parties" information item. They suggested removing the "Vulnerable customers" category due to identification challenges during the initial stages of an incident. Additionally, they proposed limiting the scope to group entities only to reduce complexities and regulatory burdens. They also suggested renaming "Affected entity" to "Affected entity types" for clarity. Minor revisions were made to clarify the scope, and the field name "Affected parties" has been changed to "Affected party types" as the field enumerates types of affected parties.

- **time of detection:** The validation rules have been adjusted to allow it to be equal to 'time of occurrence' when an incident is immediately detected at onset.

3. Other feedback received

In addition to the above feedback, the FSB received several other comments and suggestions. While these did not lead to changes to the FIRE format, the FSB provides the following responses to clarify important aspects and objectives. This selection of additional feedback highlights the need for further clarification.

- **Implementation.** Respondents emphasised the need for broad adoption and full implementation of FIRE to reduce fragmentation in cyber incident reporting and align with existing regulatory frameworks like DORA, NIS2, CER, proposed CIRCIA, and

SEC rules. They stressed avoiding additional data elements and noted the challenge of deviating from bespoke internal incident management mechanisms. The FSB acknowledges these practical challenges and the associated one-off implementation costs. A two-year period is considered reasonable to assess progress and challenges, allowing authorities and firms to adapt and gather data. Additional implementation will likely continue after this time, but the two-year review will be an important milestone to monitor progress.

- **Essential versus optional.** Respondents sought clarification on essential information items in the FIRE framework through local regulations and proposed a clearer distinction between 'Essential' and 'Optional' requirements. The FSB encourages authorities to evaluate whether and how to incorporate FIRE into their legal requirements, recognising that phased adoption can be pragmatic. FIRE is designed to be flexible and interoperable with existing frameworks, allowing authorities to customise reporting phases and provide additional specifications for unstructured fields. Partial implementation still offers coherence and interoperability benefits.

- **Adoption by third parties.** Respondents noted that broader adoption of FIRE could support third parties in reporting significant operational incidents, enhancing the response of both authorities and financial institutions. They highlighted the benefits of promoting FIRE within the supply chain for financial institutions and supported including third-party service providers in the scope of FIRE. The FSB recognises the importance of quick and effective information sharing, including with third parties, and emphasises the flexibility and interoperability of the FIRE framework, which is adaptable to existing systems.

- **Incident forwarding.** Respondents highlighted the importance of incident forwarding to facilitate information sharing and ensure traceability. The FSB clarified that including incident forwarding does not obligate authorities to forward incidents but provides clear traceability when regulations allow for it. Existing fields in FIRE can track changes and recipients without adding new fields. Bidirectional information sharing is outside the scope of FIRE and depends on each authority's powers and regulations. The scale of incidents to be reported using FIRE will be established by each reporting framework. FIRE aims to accommodate different requirements without adding unnecessary burdens, facilitating standardised and secure exchange of incident information without establishing liability protections, which are governed by individual jurisdictions.